question id	question group heading	original set name	simple_question
3492	Risk Management and Assessment	C2M2_V11	Is there a documented cybersecurity risk management strategy?
3493	Risk Management and Assessment	C2M2_V11	Does the strategy provide an approach for risk prioritization, including consideration of impact?
3494	Risk Management and Assessment	C2M2_V11	Are the organizational risk criteria defined and available?
3495	Risk Management and Assessment	C2M2_V11	Do you periodically update your risk management strategy to reflect the current threat environment?
3496	Risk Management and Assessment	C2M2_V11	Does the organization categorize and document risks and is it used in risk management activities?
3497	Risk Management and Assessment	C2M2_V11	Have cybersecurity risks been identified?
3498	Risk Management and Assessment	C2M2_V11	Are identified risks mitigated, accepted, tolerated, or transferred?
3499	Risk Management and Assessment	C2M2_V11	Are risk assessments performed to identify risks in accordance with the risk management strategy?
3500	Risk Management and Assessment	C2M2_V11	Are identified risks documented?
3501	Risk Management and Assessment	C2M2_V11	Are identified risks analyzed to prioritize response activities in accordance with the risk management strategy?
3502	Risk Management and Assessment	C2M2_V11	Are identified risks monitored in accordance with the risk management strategy?
3503	Risk Management and Assessment	C2M2_V11	Does the risk analysis process use information provided by network (IT and/or OT) architecture?
3504	Risk Management and Assessment	C2M2_V11	Does your risk management program define and use policies and procedures that implement the risk management strategy?
3505	Risk Management and Assessment	C2M2_V11	Is a recent cybersecurity architecture used to inform risk analysis?
3506	Risk Management and Assessment	C2M2_V11	Is a risk register (repository of identified risks) used to support risk management activities?
3507	Risk Management and Assessment	C2M2_V11	Are documented practices followed for risk management activities?

3508	Risk Management and Assessment	C2M2_V11	Are stakeholders for risk management activities identified and involved?
3509	Risk Management and Assessment	C2M2_V11	Are adequate resources (people, funding, and tools) provided to support risk management activities?
3510	Risk Management and Assessment	C2M2_V11	Have standards and/or guidelines been identified to inform risk management activities?
3511	Risk Management and Assessment	C2M2_V11	Are risk management activities guided by documented policies or other organizational directives?
3512	Risk Management and Assessment	C2M2_V11	Do risk management policies include compliance requirements for specified standards and/or guidelines?
3513	Risk Management and Assessment	C2M2_V11	Are risk management activities periodically reviewed to ensure conformance with policy?
3514	Risk Management and Assessment	C2M2_V11	Are responsibility and authority for the performance of risk management activities assigned to personnel?
3515	Risk Management and Assessment	C2M2_V11	Do personnel performing risk management activities have the skills and knowledge needed to perform their assigned responsibilities?
3516	Configuration Management	C2M2_V11	Is there an inventory of operations technology (OT) and information technology (IT) assets that are important to the delivery of the function?
3517	Configuration Management	C2M2_V11	Is there an inventory of information assets that are important to the delivery of the function?
3518	Configuration Management	C2M2_V11	When building an inventory of assets are information attributes to support cybersecurity strategy included?
3519	Configuration Management	C2M2_V11	Are inventoried assets prioritized based on their importance to the delivery of the function?
3520	Configuration Management	C2M2_V11	Is there an inventory for all connected information technology (IT) and operations technology (OT) assets related to the delivery of the function?
3521	Configuration Management	C2M2_V11	Is the asset inventory current and complete?
3522	Configuration Management	C2M2_V11	When it is desirable to ensure that multiple inventoried assets are configured similarly, are configuration baselines established?
3523	Configuration Management	C2M2_V11	Are configuration baselines used to configure assets at deployment?
3524	Configuration Management	C2M2_V11	Does the design of configuration baselines include cybersecurity objectives?

3525	Configuration Management	C2M2_V11	Is the configuration monitored for consistency with its baselines throughout the assets' life cycle?
3526	Configuration Management	C2M2_V11	Are configuration baselines reviewed and updated at an organizationally-defined frequency?
3527	Configuration Management	C2M2_V11	Are changes to inventoried assets evaluated before being implemented?
3528	Configuration Management	C2M2_V11	Are changes to inventoried assets logged?
3529	Configuration Management	C2M2_V11	Are changes to assets tested prior to being deployed, whenever possible?
3530	Configuration Management	C2M2_V11	Do change management practices address the full life cycle of assets?
3531	Configuration Management	C2M2_V11	Are changes to assets tested for cybersecurity impact prior to being deployed?
3532	Configuration Management	C2M2_V11	Do change logs include information about modifications that impact the cybersecurity requirements of assets?
3533	Configuration Management	C2M2_V11	Are documented practices followed for asset inventory, configuration, and change management activities?
3534	Configuration Management	C2M2_V11	Are stakeholders involved in activities such as asset inventory, configuration, and change management?
3535	Configuration Management	C2M2_V11	Are adequate resources (people, funding, and tools) provided to support asset inventory, configuration, and change management activities?
3536	Configuration Management	C2M2_V11	Have standards and/or guidelines been identified to inform asset inventory, configuration, and change management activities?
3537	Configuration Management	C2M2_V11	Are asset inventory, configuration, and change management activities guided by documented policies or other organizational directives?
3538	Configuration Management	C2M2_V11	Are asset inventory, configuration, and change management policies included in compliance requirements for specified standards and/or guidelines?
3539	Configuration Management	C2M2_V11	Are asset inventory, configuration, and change management activities periodically reviewed to ensure conformance with the policy?
3540	Configuration Management	C2M2_V11	Are responsibility and authority for the performance of asset inventory, configuration, and change management activities assigned to personnel?

3541	Configuration Management	C2M2_V11	Do personnel performing asset inventory, configuration, and change management activities have the skills and knowledge needed to perform their assigned responsibilities?
3542	Account Management	C2M2_V11	Are identities provisioned for personnel and other entities (e.g., services, devices) who require access to assets? (note that this does not preclude shared identities)
3543	Account Management	C2M2_V11	Are credentials issued for personnel and other entities that require access to assets? (e.g., passwords, smart cards, certificates, keys)
3544	Account Management	C2M2_V11	Are identities removed when no longer required?
3545	Account Management	C2M2_V11	Are identity repositories periodically reviewed and updated to ensure validity? (i.e., to ensure that the identities still need access)
3546	Account Management	C2M2_V11	Are credentials periodically reviewed to ensure that they are associated with the correct person or entity?
3547	Account Management	C2M2_V11	Are identities deprovisioned within organizationally defined time thresholds when no longer required?
3548	Account Management	C2M2_V11	Are requirements or credentials informed by the organization's risk criteria? (e.g., multifactor credentials for higher risk access)
3549	Account Management	C2M2_V11	Are access requirements determined (including those for remote access)?
3550	Account Management	C2M2_V11	Is access granted to identities based on requirements?
3551	Account Management	C2M2_V11	Is access revoked when no longer required?
3552	Account Management	C2M2_V11	Do your access requirements incorporate least privilege and separation of duties principles?
3553	Account Management	C2M2_V11	Are access requests reviewed and approved by the asset owner?
3554	Account Management	C2M2_V11	Do root privileges, administrative access, emergency access, and shared accounts receive additional scrutiny and monitoring?
3555	Account Management	C2M2_V11	Are access privileges reviewed and updated to ensure validity, at an organizationally defined frequency?
3556	Account Management	C2M2_V11	Is access to assets granted by the asset owner based on risk to the function?

3557	Account Management	C2M2_V11	Are anomalous access attempts monitored as indicators of cybersecurity events?
3558	Access Control	C2M2_V11	Are documented practices followed to establish and maintain identities and control access?
3559	Access Control	C2M2_V11	Are stakeholders identified and involved in access and identity management activities?
3560	Access Control	C2M2_V11	Are adequate resources (people, funding, and tools) provided to support access and identity management activities?
3561	Access Control	C2M2_V11	Have standards and/or guidelines been identified to inform access and identity management activities?
3562	Access Control	C2M2_V11	Are access and identity management activities guided by documented policies or other organizational directives?
3563	Access Control	C2M2_V11	Do access and identity management policies include compliance requirements for specified standards and/or guidelines?
3564	Access Control	C2M2_V11	Are access and identity management activities periodically reviewed to ensure conformance with policy?
3565	Access Control	C2M2_V11	Do personnel have responsibility and authority for the performance of access and identity management activities assigned to them?
3566	Access Control	C2M2_V11	Do personnel that are performing access and identity management activities have the skills and knowledge needed to perform their assigned responsibilities?
3567	System Integrity	C2M2_V11	Are information sources to support threat management activities identified? (e.g., US-CERT, ISACs, ICS-CERT, industry associations, vendors, federal briefings)
3568	System Integrity	C2M2_V11	Is cybersecurity threat information gathered and interpreted for the function?
3569	System Integrity	C2M2_V11	Are threats that are considered important to the function addressed? (e.g., implement mitigating controls, monitor threat status)
3570	System Integrity	C2M2_V11	Is a threat profile for the function established that includes characterization of likely intent, capability, and target of threats?
3571	System Integrity	C2M2_V11	Are threat information sources that address all components of the threat profile prioritized and monitored?
3572	System Integrity	C2M2_V11	Are identified threats analyzed and prioritized?
3573	System Integrity	C2M2_V11	Are threats addressed according to the assigned priority?
3574	System Integrity	C2M2_V11	Is the threat profile for the function validated at an organizationally-defined frequency?

3575	System Integrity	C2M2_V11	Are analysis and prioritization of threats informed by the function's or organization's risk criteria?
3576	System Integrity	C2M2_V11	Is threat information added to the risk register?
3577	System Integrity	C2M2_V11	Are information sources to support cybersecurity vulnerability discovery identified? (e.g., US-CERT, ISACs, ICS-CERT, industry associations, vendors, federal briefings, internal assessments)
3578	System Integrity	C2M2_V11	Is cybersecurity vulnerability information gathered and interpreted for the function?
3579	System Integrity	C2M2_V11	Are cybersecurity vulnerabilities which are considered important to the function addressed? (e.g., implement mitigating controls, apply cybersecurity patches)
3580	System Integrity	C2M2_V11	Are cybersecurity vulnerability information sources that address all assets important to the function monitored?
3581	System Integrity	C2M2_V11	Are cybersecurity vulnerability assessments performed? (e.g., architectural reviews, penetration testing, cybersecurity exercises, vulnerability identification tools)
3582	System Integrity	C2M2_V11	Are identified cybersecurity vulnerabilities analyzed and prioritized? (e.g., NIST Common Vulnerability Scoring System could be used for patches)
3583	System Integrity	C2M2_V11	Are cybersecurity vulnerabilities addressed according to the assigned priority?
3584	System Integrity	C2M2_V11	Is operational impact to the function evaluated prior to deploying cybersecurity patches?
3585	Risk Management and Assessment	C2M2_V11	Are cybersecurity vulnerability assessments performed for all assets important to the delivery of the function, at an organization-defined frequency?
3586	Risk Management and Assessment	C2M2_V11	Are cybersecurity vulnerability assessments informed by the function's (or organization's) risk criteria?
3587	Risk Management and Assessment	C2M2_V11	Are cybersecurity vulnerability assessments performed by parties that are independent of the operations of the function?
3588	Risk Management and Assessment	C2M2_V11	Are analysis and prioritization of cybersecurity vulnerabilities informed by the function's (or organization's) risk criteria?
3589	Risk Management and Assessment	C2M2_V11	Is cybersecurity vulnerability information added to the risk register?
3590	Risk Management and Assessment	C2M2_V11	Do risk monitoring activities validate the responses to cybersecurity vulnerabilities? (e.g., deployment of patches or other activities)
3591	System Integrity	C2M2_V11	Are documented practices followed for threat and vulnerability management activities?
3592	System Integrity	C2M2_V11	Do stakeholders identify and are they involved with threat and vulnerability management activities?

3593	System Integrity	C2M2_V11	Are adequate resources (people, funding, and tools) are provided to support threat and vulnerability management activities?
3594	System Integrity	C2M2_V11	Have standards and/or guidelines been identified to inform threat and vulnerability management activities?
3595	Monitoring & Malware	C2M2_V11	Are threat and vulnerability management activities guided by documented policies or other organizational directives?
3596	Monitoring & Malware	C2M2_V11	Do threat and vulnerability management policies include compliance requirements for specified standards and/or guidelines?
3597	Monitoring & Malware	C2M2_V11	Are threat and vulnerability management activities periodically reviewed to ensure conformance with policy?
3598	Monitoring & Malware	C2M2_V11	Are responsibility and authority for the performance of threat and vulnerability management activities assigned to personnel?
3599	Monitoring & Malware	C2M2_V11	Do personnel performing threat and vulnerability management activities have the skills and knowledge needed to perform their assigned responsibilities?
3600	Audit and Accountability	C2M2_V11	Are logs being generated for assets important to the function where possible?
3601	Audit and Accountability	C2M2_V11	Have logging requirements been defined for all assets important to the function? (e.g., scope of activity and coverage of assets, cybersecurity requirements [confidentiality, integrity, availability])
3602	Audit and Accountability	C2M2_V11	Are log data being aggregated within the function?
3603	Audit and Accountability	C2M2_V11	Are logging requirements based on risk to the function?
3604	Audit and Accountability	C2M2_V11	Does log data support other business and security processes? (e.g., incident response, asset management)
3605	Audit and Accountability	C2M2_V11	Are cybersecurity monitoring activities performed? (e.g., periodic reviews of log data)
3606	Audit and Accountability	C2M2_V11	Are operational environments monitored for anomalous behavior that may indicate a cybersecurity event?
3607	Audit and Accountability	C2M2_V11	Have monitoring and analysis requirements been defined for the function and address timely review of event data?
3608	Audit and Accountability	C2M2_V11	Are alarms and alerts configured to aid in the identification of cybersecurity events?

3609	Audit and Accountability	C2M2_V11	Have indicators of anomalous activity been defined and are monitored across the operational environment?
3610	Audit and Accountability	C2M2_V11	Are monitoring activities aligned with the function's threat profile?
3611	Audit and Accountability	C2M2_V11	Are monitoring requirements based on the risk to the function?
3612	Audit and Accountability	C2M2_V11	Is monitoring integrated with other business and security processes? (e.g., incident response, asset management)
3613	Audit and Accountability	C2M2_V11	Is continuous monitoring performed across the operational environment to identify anomalous activity?
3614	Audit and Accountability	C2M2_V11	Is risk register (a structured repository of identified risks. See RM-2j) content used to identify indicators of anomalous activity?
3615	Audit and Accountability	C2M2_V11	Are alarms and alerts configured according to indicators of anomalous activity?
3616	System Integrity	C2M2_V11	Are methods of communicating the current cybersecurity state for the function established and maintained?
3617	System Integrity	C2M2_V11	Are monitoring data aggregated to provide an understanding of the operational state of the function? (i.e., a common operating picture (COP) which may or may not include visualization or be presented graphically)
3618	System Integrity	C2M2_V11	Is information from across the organization available to enhance the common operating picture?
3619	System Integrity	C2M2_V11	Are aggregated monitoring data used to provide near-real-time understanding of the cybersecurity state for the function in order to enhance the common operating picture?
3620	System Integrity	C2M2_V11	Is information from outside the organization collected to enhance the common operating picture?
3621	System Integrity	C2M2_V11	Are predefined states of operation defined and invoked (manual or automated) based on the common operating picture?
3622	System Integrity	C2M2_V11	Are documented practices followed for logging, monitoring, and COP activities?
3623	System Integrity	C2M2_V11	Are stakeholders identified and become involved in logging, monitoring, and COP activities?
3624	System Integrity	C2M2_V11	Are adequate resources (people, funding, and tools) provided to support logging, monitoring, and COP activities?

3625	System Integrity	C2M2_V11	Have standards and/or guidelines been identified to inform logging, monitoring, and COP activities?
3626	System Integrity	C2M2_V11	Are logging, monitoring, and COP activities guided by documented policies or other organizational directives?
3627	System Integrity	C2M2_V11	Do logging, monitoring, and COP policies include compliance requirements for specified standards and/or guidelines?
3628	System Integrity	C2M2_V11	Are logging, monitoring, and COP activities periodically reviewed to ensure conformance with policy?
3629	System Integrity	C2M2_V11	Are responsibility and authority for the performance of logging, monitoring, and COP activities assigned to personnel?
3630	System Integrity	C2M2_V11	Do personnel performing logging, monitoring, and COP activities have the skills and knowledge needed to perform their assigned responsibilities?
3631	System Integrity	C2M2_V11	Is information collected from and provided to selected individuals and/or organizations?
3632	System Integrity	C2M2_V11	Is the responsibility for cybersecurity reporting assigned to personnel? (e.g., internal reporting, ICS-CERT, law enforcement)
3633	System Integrity	C2M2_V11	Are information-sharing stakeholders identified based on their relevance to the continued operation of the function? (e.g., connected organizations, vendors, sector organizations, regulators, internal entities)
3634	System Integrity	C2M2_V11	Is information collected from and provided to identified information-sharing stakeholders?
3635	System Integrity	C2M2_V11	Are technical sources identified that can be consulted on cybersecurity issues?
3636	System Integrity	C2M2_V11	Are provisions established and maintained to enable secure sharing of sensitive or classified information?
3637	System Integrity	C2M2_V11	Do information-sharing practices address standard and emergency operations?
3638	System Integrity	C2M2_V11	Are information-sharing stakeholders identified based on shared interest and risk to critical infrastructure?
3639	System Integrity	C2M2_V11	Does the function or the organization participate with information sharing and analysis centers?
3640	System Integrity	C2M2_V11	Have information-sharing requirements and the timely dissemination of cybersecurity information for the function been defined and addressed?
3641	System Integrity	C2M2_V11	Are procedures in place to analyze and coordinate received information?
3642	System Integrity	C2M2_V11	Have a network of internal and external trust relationships (formal and/or informal) been established to vet and validate cyber events?

3643	System Integrity	C2M2_V11	Are documented practices followed for information-sharing activities?
3644	System Integrity	C2M2_V11	Are stakeholders for information-sharing activities identified and involved?
3645	System Integrity	C2M2_V11	Are adequate resources (people, funding, and tools) provided to support information-sharing activities?
3646	System Integrity	C2M2_V11	Have standards and/or guidelines been identified to inform information-sharing activities?
3647	System Integrity	C2M2_V11	Are information-sharing activities guided by documented policies or other organizational directives?
3648	System Integrity	C2M2_V11	Do information-sharing policies include compliance requirements for specified standards and/or guidelines?
3649	System Integrity	C2M2_V11	Are information-sharing activities periodically reviewed to ensure conformance with policy?
3650	System Integrity	C2M2_V11	Are responsibility and authority for the performance of information-sharing activities assigned to personnel?
3651	System Integrity	C2M2_V11	Do personnel performing information-sharing activities have the skills and knowledge needed to perform their assigned responsibilities?
3652	System Integrity	C2M2_V11	Do information-sharing policies address protected information and ethical use and sharing of information, including sensitive and classified information as appropriate?
3653	Incident Response	C2M2_V11	Is there a point of contact (person or role) to whom cybersecurity events could be reported?
3654	Incident Response	C2M2_V11	Are detected cybersecurity events reported?
3655	Incident Response	C2M2_V11	Are cybersecurity events logged and tracked?
3656	Incident Response	C2M2_V11	Are criteria established for cybersecurity event detection? (e.g., what constitutes an event, where to look for events)
3657	Incident Response	C2M2_V11	Is there a repository where cybersecurity events are logged based on the established criteria?
3658	Incident Response	C2M2_V11	Is event information correlated to support incident analysis by identifying patterns, trends, and other common features?
3659	Incident Response	C2M2_V11	Are cybersecurity event detection activities adjusted based on information from the organization's risk register (a structured repository of identified risks, see RM-2j) and threat profile (including characterization of likely intent, capability, and target of threats to the function, see TVM-1d) to help detect known threats and monitor for identified risks?

3660	Incident Response	C2M2_V11	Is the common operating picture for the function monitored to support the identification of cybersecurity events?
3661	Incident Response	C2M2_V11	Are criteria for cybersecurity event escalation established, including cybersecurity incident declaration criteria?
3662	Incident Response	C2M2_V11	Are cybersecurity events analyzed to support escalation and the declaration of cybersecurity incidents?
3663	Incident Response	C2M2_V11	Are escalated cybersecurity events and incidents logged and tracked?
3664	Incident Response	C2M2_V11	Are criteria for cybersecurity event escalation (including cybersecurity incident criteria) established based on the potential impact to the function?
3665	Incident Response	C2M2_V11	Are criteria for cybersecurity event escalation (including cybersecurity incident declaration criteria) updated at an organizationally-defined frequency?
3666	Incident Response	C2M2_V11	Is there a repository where escalated cybersecurity events and incidents are logged and tracked to closure?
3667	Incident Response	C2M2_V11	Are criteria for cybersecurity event escalation (including cybersecurity incident declaration criteria) adjusted according to information from the organization's risk register (RM-2j) and threat profile (TVM-1d)?
3668	Incident Response	C2M2_V11	Do escalated cybersecurity events and declared cybersecurity incidents inform the common operating picture (COP) (SA-3a) for the function?
3669	Incident Response	C2M2_V11	Are escalated cybersecurity events and declared incidents correlated to support the discovery of patterns, trends, and other common features?
3670	Incident Response	C2M2_V11	Are cybersecurity event and incident response personnel identified and roles assigned?
3671	Incident Response	C2M2_V11	Are responses to escalated cybersecurity events and incidents implemented to limit impact to the function and restore normal operations?
3672	Incident Response	C2M2_V11	Is reporting of escalated cybersecurity events and incidents performed? (e.g., internal reporting, ICS-CERT, relevant ISACs)
3673	Incident Response	C2M2_V11	Is cybersecurity event and incident response performed according to defined procedures that address all phases of the incident life cycle? (e.g., triage, handling, communication, coordination, and closure)
3674	Incident Response	C2M2_V11	Are cybersecurity event and incident response plans exercised at an organizationally-defined frequency?
3675	Incident Response	C2M2_V11	Do cybersecurity event and incident response plans address information technology (IT) and operations technology (OT) assets important to the delivery of the function?
3676	Incident Response	C2M2_V11	Is training conducted for cybersecurity event and incident response teams?

3677	Incident Response	C2M2_V11	Are cybersecurity event and incident root-cause analysis and lessons-learned activities performed, and corrective actions taken?
3678	Incident Response	C2M2_V11	Are cybersecurity event and incident responses coordinated with law enforcement and other government entities as appropriate, including support for evidence collection and preservation?
3679	Incident Response	C2M2_V11	Do cybersecurity event and incident response personnel participate in joint cybersecurity exercises with other organizations? (e.g., table top, simulated incidents)
3680	Incident Response	C2M2_V11	Are cybersecurity event and incident response plans reviewed and updated at an organizationally-defined frequency?
3681	Incident Response	C2M2_V11	Are cybersecurity event and incident response activities coordinated with relevant external entities?
3682	Incident Response	C2M2_V11	Are cybersecurity event and incident response plans aligned with the function's risk criteria (RM-1c) and threat profile (TVM-1d)?
3683	Incident Response	C2M2_V11	Do policies and procedures for reporting cybersecurity event and incident information to designated authorities conform with applicable laws, regulations, and contractual agreements?
3684	Incident Response	C2M2_V11	Are restored assets configured appropriately and inventory information updated following execution of response plans?
3685	Continuity	C2M2_V11	Are the necessary activities identified to sustain minimum operations of the function?
3686	Continuity	C2M2_V11	Is the sequence of necessary activities identified to return the function to normal operation?
3687	Continuity	C2M2_V11	Are continuity plans developed to sustain and restore operation of the function?
3688	Continuity	C2M2_V11	Do business impact analyses inform the development of continuity plans?
3689	Continuity	C2M2_V11	Are recovery time objectives (RTO) and recovery point objectives (RPO) for the function incorporated into continuity plans?
3690	Continuity	C2M2_V11	Are continuity plans evaluated and exercised?
3691	Continuity	C2M2_V11	Are business impact analyses periodically reviewed and updated?
3692	Continuity	C2M2_V11	Are recovery time objective (RTO) and recovery point objectives (RPO) aligned with the function's risk criteria (objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, tolerance for risk, and risk response approaches, see RM-1c)?

3693	Continuity	C2M2_V11	Are the results of continuity plan testing and/or activation compared to recovery objectives, and plans are improved accordingly?
3694	Continuity	C2M2_V11	Are continuity plans periodically reviewed and updated?
3695	Continuity	C2M2_V11	Are restored assets configured appropriately and inventory information updated following execution of the continuity plans?
3696	Continuity	C2M2_V11	Are documented practices followed for cybersecurity event and incident response as well as continuity of operations activities?
3697	Continuity	C2M2_V11	Are stakeholders for cybersecurity event and incident response as well as continuity of operations activities identified and involved?
3698	Continuity	C2M2_V11	Are adequate resources (people, funding, and tools) provided to support cybersecurity event and incident response as well as continuity of operations activities?
3699	Continuity	C2M2_V11	Have standards and/or guidelines been identified to inform cybersecurity event and incident response as well as continuity of operations activities?
3700	Continuity	C2M2_V11	Are cybersecurity event and incident response as well as continuity of operations activities guided by documented policies or other organizational directives?
3701	Continuity	C2M2_V11	Do cybersecurity event and incident response as well as continuity of operations policies include compliance requirements for specified standards and/or guidelines?
3702	Continuity	C2M2_V11	Are cybersecurity event and incident response as well as continuity of operations activities periodically reviewed to ensure conformance with policy?
3703	Continuity	C2M2_V11	Are responsibility and authority for the performance of cybersecurity event and incident response as well as continuity of operations activities assigned to personnel?
3704	Continuity	C2M2_V11	Do personnel performing cybersecurity event and incident response as well as continuity of operations activities have the skills and knowledge needed to perform their assigned responsibilities?
3705	System and Services Acquisition	C2M2_V11	Are important information technology (IT) and operations technology (OT) supplier dependencies identified? (e.g., external parties on which the delivery of the function depend, including operating partners)
3706	System and Services Acquisition	C2M2_V11	Are important customer dependencies identified? (e.g., external parties that are dependent on the delivery of the function, including operating partners)
3707	System and Services Acquisition	C2M2_V11	Are supplier dependencies identified according to established criteria?

3708	System and Services Acquisition	C2M2_V11	Are customer dependencies identified according to established criteria?
3709	System and Services Acquisition	C2M2_V11	Are single source and other essential dependencies identified?
3710	System and Services Acquisition	C2M2_V11	Are dependencies prioritized?
3711	System and Services Acquisition	C2M2_V11	Is dependency prioritization and identification based on the function's or organization's risk criteria (RM-1c)?
3712	System and Services Acquisition	C2M2_V11	Are significant cybersecurity risks due to suppliers and other dependencies identified and addressed?
3713	System and Services Acquisition	C2M2_V11	Are cybersecurity requirements considered when establishing relationships with suppliers and other third parties?
3714	System and Services Acquisition	C2M2_V11	Are identified cybersecurity dependency risks entered into the risk register (RM-2j)?
3715	System and Services Acquisition	C2M2_V11	Do contracts and agreements with third parties incorporate sharing of cybersecurity threat information?
3716	System and Services Acquisition	C2M2_V11	Are cybersecurity requirements established for suppliers according to a defined practice, including requirements for secure software development practices where appropriate?
3717	System and Services Acquisition	C2M2_V11	Do agreements with suppliers and other external entities include cybersecurity requirements?
3718	System and Services Acquisition	C2M2_V11	Do evaluation and selection of suppliers and other external entities include consideration of their ability to meet cybersecurity requirements?
3719	System and Services Acquisition	C2M2_V11	Do agreements with suppliers require notification of cybersecurity incidents related to the delivery of the product or service?
3720	System and Services Acquisition	C2M2_V11	Are suppliers and other external entities periodically reviewed for their ability to continually meet the cybersecurity requirements?
3721	System and Services Acquisition	C2M2_V11	Are cybersecurity risks due to external dependencies managed according to the organization's risk management criteria and process?
3722	System and Services Acquisition	C2M2_V11	Are cybersecurity requirements established for supplier dependencies based on the organization's risk criteria (RM-1c)?
3723	System and Services Acquisition	C2M2_V11	Do agreements with suppliers require notification of vulnerability-inducing product defects throughout the intended life cycle of delivered products?

3724	System and Services Acquisition	C2M2_V11	Does acceptance testing of procured assets include testing for cybersecurity requirements?
3725	System and Services Acquisition	C2M2_V11	Are information sources monitored to identify and avoid supply chain threats? (e.g., counterfeit parts, software, and services)
3726	System and Services Acquisition	C2M2_V11	Are documented practices followed for managing dependency risk?
3727	System and Services Acquisition	C2M2_V11	Are stakeholders for managing dependency risk identified and involved?
3728	System and Services Acquisition	C2M2_V11	Are adequate resources (people, funding, and tools) provided to support dependency risk management activities?
3729	System and Services Acquisition	C2M2_V11	Have standards and/or guidelines been identified to inform managing dependency risk?
3730	System and Services Acquisition	C2M2_V11	Are dependency risk management activities guided by documented policies or other organizational directives?
3731	System and Services Acquisition	C2M2_V11	Do dependency risk management policies include compliance requirements for specified standards and/or guidelines?
3732	System and Services Acquisition	C2M2_V11	Are dependency risk management activities periodically reviewed to ensure conformance with policy?
3733	System and Services Acquisition	C2M2_V11	Are responsibility and authority for the performance of dependency risk management assigned to personnel?
3734	System and Services Acquisition	C2M2_V11	Do personnel performing dependency risk management have the skills and knowledge needed to perform their assigned responsibilities?
3735	Organizational	C2M2_V11	Are cybersecurity responsibilities for the function identified?
3736	Organizational	C2M2_V11	Are cybersecurity responsibilities assigned to specific people?
3737	Organizational	C2M2_V11	Are cybersecurity responsibilities assigned to specific roles, including external service providers?
3738	Organizational	C2M2_V11	Are cybersecurity responsibilities documented? (e.g., in position descriptions)
3739	Organizational	C2M2_V11	Are cybersecurity responsibilities and job requirements reviewed and updated as appropriate?
3740	Organizational	C2M2_V11	Are cybersecurity responsibilities included in job performance evaluation criteria?
3741	Organizational	C2M2_V11	Are assigned cybersecurity responsibilities managed to ensure adequacy and redundancy of coverage?
3742	Personnel	C2M2_V11	Is personnel vetting (e.g., background checks, drug tests) performed at hire for positions that have access to the assets required for delivery of the function?

3743	Personnel	C2M2_V11	Do personnel termination procedures address cybersecurity?
3744	Personnel	C2M2_V11	Is personnel vetting performed at an organizationally-defined frequency for positions that have access to the assets required for delivery of the function?
3745	Personnel	C2M2_V11	Do personnel transfer procedures address cybersecurity?
3746	Personnel	C2M2_V11	Are risk designations assigned to all positions that have access to the assets required for delivery of the function?
3747	Personnel	C2M2_V11	Is vetting performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk designation?
3748	Personnel	C2M2_V11	Is succession planning performed for personnel based on risk designation?
3749	Personnel	C2M2_V11	Is a formal accountability process (including disciplinary actions) implemented for personnel who fail to comply with established security policies and procedures?
3750	Training	C2M2_V11	Is cybersecurity training made available to personnel with assigned cybersecurity responsibilities?
3751	Training	C2M2_V11	Are cybersecurity knowledge, skill, and ability gaps identified?
3752	Training	C2M2_V11	Are identified gaps addressed through recruiting and/or training?
3753	Training	C2M2_V11	Is cybersecurity training provided as a prerequisite to granting access to assets that support the delivery of the function? (e.g., new personnel training, personnel transfer training)
3754	Training	C2M2_V11	Are cybersecurity workforce management objectives that support current and future operational needs established and maintained?
3755	Training	C2M2_V11	Are recruiting and retention aligned to support cybersecurity workforce management objectives?
3756	Training	C2M2_V11	Are training programs aligned to support cybersecurity workforce management objectives?
3757	Training	C2M2_V11	Is the effectiveness of training programs evaluated at an organizationally-defined frequency and are improvements made as appropriate?
3758	Training	C2M2_V11	Do training programs include continuing education and professional development opportunities for personnel with significant cybersecurity responsibilities?
3759	Training	C2M2_V11	Do any cybersecurity awareness activities occur?
3760	Training	C2M2_V11	Are objectives for cybersecurity awareness activities established and maintained?
3761	Training	C2M2_V11	Is cybersecurity awareness content based on the organization's threat profile (TVM-1d)?
3762	Training	C2M2_V11	Are cybersecurity awareness activities aligned with the predefined states of operation (SA-3f)?

3763	Training	C2M2_V11	Is the effectiveness of cybersecurity awareness activities evaluated at an organizationally-defined frequency and are improvements made as appropriate?
3764	Incident Response	C2M2_V11	Are documented practices followed for cybersecurity workforce management activities?
3765	Incident Response	C2M2_V11	Are stakeholders for cybersecurity workforce management activities identified and involved?
3766	Incident Response	C2M2_V11	Are adequate resources (people, funding, and tools) provided to support cybersecurity workforce management activities?
3767	Incident Response	C2M2_V11	Have standards and/or guidelines been identified to inform cybersecurity workforce management activities?
3768	Incident Response	C2M2_V11	Are cybersecurity workforce management activities guided by documented policies or other organizational directives?
3769	Incident Response	C2M2_V11	Do cybersecurity workforce management policies include compliance requirements for specified standards and/or guidelines?
3770	Incident Response	C2M2_V11	Are cybersecurity workforce management activities periodically reviewed to ensure conformance with policy?
3771	Incident Response	C2M2_V11	Are responsibility and authority for the performance of cybersecurity workforce management activities assigned to personnel?
3772	Incident Response	C2M2_V11	Do personnel performing cybersecurity workforce management activities have the skills and knowledge needed to perform their assigned responsibilities?
3773	Policies & Procedures General	C2M2_V11	Does the organization have a cybersecurity program strategy?
3774	Policies & Procedures General	C2M2_V11	Does the cybersecurity program strategy define objectives for the organization's cybersecurity activities?
3775	Policies & Procedures General	C2M2_V11	Are the cybersecurity program strategy and priorities documented and aligned with the organization's strategic objectives and risk to critical infrastructure?
3776	Policies & Procedures General	C2M2_V11	Does the cybersecurity program strategy define the organization's approach to provide program oversight and governance for cybersecurity activities?
3777	Policies & Procedures General	C2M2_V11	Does the cybersecurity program strategy define the structure and organization of the cybersecurity program?
3778	Policies & Procedures General	C2M2_V11	Is the cybersecurity program strategy approved by senior management?
3779	Policies & Procedures General	C2M2_V11	Is the cybersecurity program strategy updated to reflect business changes, changes in the operating environment, and changes in the threat profile (TVM-1d)?

3780	Organizational	C2M2_V11	Are resources (people, tools, and funding) provided to support the cybersecurity program?
3781	Organizational	C2M2_V11	Does senior management provide sponsorship for the cybersecurity program?
3782	Organizational	C2M2_V11	Is the cybersecurity program established according to the cybersecurity program strategy?
3783	Organizational	C2M2_V11	Are adequate funding and other resources (e.g., people and tools) provided to establish and operate a cybersecurity program aligned with the program strategy?
3784	Organizational	C2M2_V11	Is senior management sponsorship for the cybersecurity program visible and active? (i.e., the importance and value of cybersecurity activities is regularly communicated by senior management)
3785	Organizational	C2M2_V11	If the organization develops or procures software, are secure software development practices sponsored as an element of the cybersecurity program?
3786	Organizational	C2M2_V11	Is the development and maintenance of cybersecurity policies sponsored?
3787	Organizational	C2M2_V11	Is responsibility for the cybersecurity program assigned to a role with requisite authority?
3788	Organizational	C2M2_V11	Is the performance of the cybersecurity program monitored to ensure it aligns with the cybersecurity program strategy?
3789	Organizational	C2M2_V11	Is the cybersecurity program independently reviewed for achievement of cybersecurity program objectives? (i.e., by reviewers who are not in the program)
3790	Organizational	C2M2_V11	Does the cybersecurity program address and enable the achievement of regulatory compliance as appropriate?
3791	Organizational	C2M2_V11	Does the cybersecurity program monitor and/or participate in selected industry cybersecurity standards or initiatives?
3792	Organizational	C2M2_V11	Is a strategy to architecturally isolate the organization's IT systems from OT systems implemented?
3793	System Protection	C2M2_V11	Is a cybersecurity architecture in place to enable segmentation, isolation, and other requirements that support the cybersecurity strategy?
3794	System Protection	C2M2_V11	Is architectural segmentation and isolation maintained according to a documented plan?
3795	Organizational	C2M2_V11	Is cybersecurity architecture updated at an organizationally-defined frequency?
3796	System Integrity	C2M2_V11	Is software to be deployed on assets that are important to the delivery of the function developed using secure software development practices?

3797	System Integrity	C2M2_V11	Do policies require that software that is to be deployed on assets that are important to the delivery of the function be developed using secure software development practices?
3798	Organizational	C2M2_V11	Are documented practices followed for cybersecurity program management activities?
3799	Organizational	C2M2_V11	Are stakeholders for cybersecurity program management activities identified and involved?
3800	Organizational	C2M2_V11	Have standards and/or guidelines been identified to inform cybersecurity program management activities?
3801	Organizational	C2M2_V11	Are cybersecurity program management activities guided by documented policies or other organizational directives?
3802	Organizational	C2M2_V11	Are cybersecurity program management activities periodically reviewed to ensure conformance with policy?
3803	Organizational	C2M2_V11	Do personnel performing cybersecurity program management activities have the skills and knowledge needed to perform their assigned responsibilities?
1259	Account Management	C800_53_R3	Are users required to log out when a defined time-period of expected inactivity and/or description of when to log out?
1260	Account Management	C800_53_R3	Is the normal time-of-day and duration usage for accounts determined?
1261	Account Management	C800_53_R3	Is the atypical usage of accounts monitored?
1262	Account Management	C800_53_R3	Is the atypical usage of accounts reported to designated officials?
1263	Account Management	C800_53_R3	Are user privileges and associated access authorizations dynamically managed?
1269	Account Management	C800_53_R3	Is the separation of duties documented?
1270	Access Control	C800_53_R3	Is the authorization to super user accounts limited to designated system administration personnel?
1271	Access Control	C800_53_R3	Is the privileged access to the system prohibited for nonorganizational users?
1272	Access Control	C800_53_R3	Does the system purge information from mobile devices after a defined number of consecutive, unsuccessful login attempts to the device?

1273	Portable/Mobile/Wireless	C800_53_R3	Is the system monitored for unauthorized wireless connections? Does the monitoring include scanning for unauthorized wireless access points on defined frequency, and is appropriate action taken if an unauthorized connection is discovered?
1274	Portable/Mobile/Wireless	C800_53_R3	Are wireless communications confined to organization-controlled boundaries?
1275	Training	C800_53_R3	Are employees provided with initial and periodic training in the employment and operation of environmental controls?
1276	Training	C800_53_R3	Are employees provided with initial and periodic training in the employment and operation of physical security controls?
1277	Audit and Accountability	C800_53_R3	Does the system shut down in the event of an audit failure, unless an alternative audit capability exists?
1278	Audit and Accountability	C800_53_R3	Is information from audit records correlated with information from monitoring physical access to identify suspicious, inappropriate, unusual, or malevolent activity?
1279	Audit and Accountability	C800_53_R3	Are the permitted actions specified for each authorized information system process, role, and/or user in the audit and accountability policy?
1280	Audit and Accountability	C800_53_R3	Are automated mechanisms used to alert security personnel of a defined list of inappropriate or unusual activities?
1281	Audit and Accountability	C800_53_R3	Is full-text analysis of privileged functions executed performed in a physically dedicated system?
1282	Audit and Accountability	C800_53_R3	Are cryptographic mechanisms used to protect the integrity of audit information and audit tools?
1283	Audit and Accountability	C800_53_R3	Is access to management of audit functionality authorized only to a limited subset of privileged users? Are audit records of nonlocal accesses to privileged accounts and the execution of privileged functions protected?
1284	Audit and Accountability	C800_53_R3	Does the system protect against an individual falsely denying having performed a particular action?
1285	Audit and Accountability	C800_53_R3	Is the identity of the information producer associated with the information?
1286	Audit and Accountability	C800_53_R3	Does the system validate the binding of the information producer's identity to the information?
1287	Audit and Accountability	C800_53_R3	Are reviewer/releaser identity and credentials maintained within the established chain of custody for all information reviewed or released?

1288	Audit and Accountability	C800_53_R3	Does the system validate the binding of the reviewer's identity to the information at the transfer/release point prior to release/transfer from one security domain to another security domain?
1289	Audit and Accountability	C800_53_R3	Is FIPS-validated or NSA-approved cryptography used to implement digital signatures?
1290	Audit and Accountability	C800_53_R3	Is a systemwide audit trail produced and composed of audit records in a standardized format?
1291	Audit and Accountability	C800_53_R3	Are session audits initiated at system startup?
1292	Risk Management and Assessment	C800_53_R3	Does the security assessment plan describe the scope of the assessment and include the security controls and control enhancements under assessment, the assessment procedures to be used, the assessment environment, the assessment team, and assessment roles and responsibilities?
1293	Risk Management and Assessment	C800_53_R3	Are the written results of the security control assessment provided to the authorizing official or designated representative?
1294	Risk Management and Assessment	C800_53_R3	Is the direct connection of an unclassified national security system prohibited to an external network?
1295	Risk Management and Assessment	C800_53_R3	Is the direct connection of a classified national security system prohibited to an external network?
1296	Plans	C800_53_R3	Are automated mechanisms used to help ensure that the plan of action and milestones for the system are accurate, up to date, and readily available?
1297	Organizational	C800_53_R3	Is the security authorization updated on a defined frequency?
1298	Risk Management and Assessment	C800_53_R3	Does the continuous monitoring program include ongoing security control assessments in accordance with the organizational continuous monitoring strategy?
1299	Configuration Management	C800_53_R3	Are older versions of baseline configurations retained as necessary to support rollback?
1300	Configuration Management	C800_53_R3	Is there a defined list of software programs not authorized to execute on the system? Is the authorization policy an allow-all, deny-by-exception for software allowed to execute on the system?
1301	Configuration Management	C800_53_R3	Are configuration-controlled changes to the system approved with explicit consideration for security impact analyses?
1302	Configuration Management	C800_53_R3	Are configuration change control activities provided and coordinated through a defined configuration change control element that convenes on a defined frequency or for defined configuration change conditions?

1303	Configuration Management	C800_53_R3	Does the configuration change control element have a security representative member?
1304	Configuration Management	C800_53_R3	Are the security functions checked after any system changes to verify that the functions are implemented correctly, operating as intended, and meeting the security requirements for the system?
1305	Configuration Management	C800_53_R3	Are the privileges to change software resident within software libraries limited?
1306	Configuration Management	C800_53_R3	Is conformance to security configuration guidance demonstrated prior to being introduced into a production environment?
1307	System Protection	C800_53_R3	Are there defined registration requirements for ports, protocols, and services?
1308	Configuration Management	C800_53_R3	Is there an inventory of system components that is available for review and audit by organizational officials?
1309	Policies & Procedures General	C800_53_R3	Is there a formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance?
1310	Plans	C800_53_R3	Is the contingency plan distributed to a defined list of key contingency personnel and organizational elements?
1311	Plans	C800_53_R3	Are contingency plan changes communicated to a defined list of key contingency personnel and organizational elements?
1312	Plans	C800_53_R3	Has capacity planning determined the necessary capacity for information processing, telecommunications, and environmental support needed during contingency operations?
1313	Plans	C800_53_R3	Is the resumption of essential missions and business functions planned for within a defined time period of contingency plan activation?
1314	Plans	C800_53_R3	Is a full recovery and reconstitution of the system to a known state included as part of contingency plan testing?
1315	Continuity	C800_53_R3	Are the backups of system documentation, including security-related documentation, done on a defined frequency consistent with recovery time and recovery point objectives?
1316	Continuity	C800_53_R3	Is system backup information transferred to the alternate storage site on a defined time period, and is the transfer rate consistent with the recovery time and recovery point objectives?
1317	Continuity	C800_53_R3	Is a redundant secondary system that is not co-located used for system backup, and can it be activated without loss of information or disruption to the operation?

1318	Access Control	C800_53_R3	Is multifactor authentication used for network access to nonprivileged accounts?
1319	Access Control	C800_53_R3	Is multifactor authentication used for local access to nonprivileged accounts?
1320	Access Control	C800_53_R3	Is multifactor authentication used for network access to nonprivileged accounts where one of the factors is provided by a device separate from the system being accessed?
1321	Access Control	C800_53_R3	Are defined replay-resistant authentication mechanisms used for network access to privileged accounts? (e.g., Kerberos, LDAP, etc.)
1322	Access Control	C800_53_R3	Are defined replay-resistant authentication mechanisms used for network access to nonprivileged accounts?
1323	Access Control	C800_53_R3	Does the organization standardize, with regard to dynamic address allocation, Dynamic Host Control Protocol (DHCP) lease information and the time assigned to devices, and audit lease information when assigned to a device?
1324	Account Management	C800_53_R3	Do user identifiers uniquely identify the user by a defined characteristic identifying user status?
1325	Account Management	C800_53_R3	Are identifiers, attributes, and associated access authorizations dynamically managed?
1326	Account Management	C800_53_R3	Is there a minimum password complexity of defined requirements for case sensitivity, number of characters, mix of upper case letters, lower case letters, numbers, and special characters, including minimum requirements for each type?
1327	Account Management	C800_53_R3	Do new passwords require a defined number of changed characters?
1328	Account Management	C800_53_R3	Are passwords encrypted in storage and in transmission?
1329	Account Management	C800_53_R3	Is there a defined minimum and maximum lifetime restriction for passwords?
1330	Account Management	C800_53_R3	Is password reuse prohibited for a defined number of generations?
1331	Account Management	C800_53_R3	Are defined measures taken to manage the risk of compromise due to individuals having accounts on multiple systems?
1332	Incident Response	C800_53_R3	Is the system dynamically reconfigured as part of the incident response capability?
1333	Incident Response	C800_53_R3	Are classes of incidents identified, and are appropriate actions defined to ensure continuation of organizational missions and business functions?
1334	Incident Response	C800_53_R3	Are personnel required to report suspected security incidents to the organizational incident response authority within a defined time-period?

1335	Maintenance	C800_53_R3	Are there procedures for the use of maintenance personnel that lack appropriate security clearances or for non - U.S. citizens?
1336	Maintenance	C800_53_R3	Are maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals escorted and supervised during the performance of maintenance and diagnostic activities on the system by approved personnel who are fully cleared, have appropriate access authorizations, and are technically qualified?
1337	Maintenance	C800_53_R3	Are all volatile information storage components within the system sanitized, and are all nonvolatile storage media removed or physically disconnected from the system and secured before initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals?
1338	Maintenance	C800_53_R3	Are the procedures contained in the security plan for the system enforced when a system component cannot be sanitized?
1339	Maintenance	C800_53_R3	Are all personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information cleared for the highest level of information on the system?
1340	Maintenance	C800_53_R3	Are all personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information U.S. citizens?
1341	Maintenance	C800_53_R3	Are cleared foreign nationals used to conduct maintenance and diagnostic activities on a system only when the system is jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments?
1342	Maintenance	C800_53_R3	Are the approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on a system fully documented with a Memorandum of Agreement?
1343	Info Protection	C800_53_R3	Are cryptographic mechanisms used to protect and restrict access to information on portable digital media?
1344	Info Protection	C800_53_R3	Are cryptographic mechanisms used to protect information in storage?
1345	Info Protection	C800_53_R3	Are cryptographic mechanisms used to protect digital media during transport outside of controlled areas?
1346	Info Protection	C800_53_R3	Are the circumstances defined where portable, removable storage devices are required to be sanitized prior to connection to the system?

1347	Info Protection	C800_53_R3	Is system media containing Controlled Unclassified Information (CUI) or other sensitive information sanitized in accordance with applicable organizational and/or federal standards and policies?
1348	Info Protection	C800_53_R3	Is system media containing classified information sanitized in accordance with NSA standards and policies?
1349	Info Protection	C800_53_R3	Is system media that cannot be sanitized destroyed?
1350	Physical Security	C800_53_R3	Is the physical access to the facility containing a system that processes classified information restricted to authorized personnel with appropriate clearances and access authorizations?
1351	Physical Security	C800_53_R3	Is the physical tampering or alteration of hardware components within the system detected or prevented?
1352	Physical Security	C800_53_R3	The organization controls physical access to information system distribution and transmission lines within organizational facilities.
1353	Environmental Security	C800_53_R3	Does the facility undergo fire marshal inspections on a defined frequency, and are identified deficiencies promptly resolved?
1354	Environmental Security	C800_53_R3	Are automatic temperature and humidity controls used to prevent fluctuations potentially harmful to the system?
1355	Environmental Security	C800_53_R3	Does temperature and humidity monitoring provide an alarm or notification of changes potentially harmful to personnel or equipment?
1356	Continuity	C800_53_R3	Is the effectiveness of security controls at alternate work sites assessed?
1357	Communication Protection	C800_53_R3	Are system components, associated data communications, and networks protected in accordance with National emissions and TEMPEST policies and procedures, and the sensitivity of the information being transmitted?
1358	Organizational	C800_53_R3	Is there a security Concept of Operations for the system that contains the purpose of the system, a description of the system architecture, the security authorization schedule, and the security categorization and associated factors considered in determining the categorization?
1359	Organizational	C800_53_R3	Is the Conduct of Operations reviewed and updated on a defined frequency?
1360	Organizational	C800_53_R3	Is there a functional architecture for the system?
1361	Organizational	C800_53_R3	Does the functional architecture define the external interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface?
1362	Organizational	C800_53_R3	Does the functional architecture define the user roles and the access privileges assigned to each role?

1363	Organizational	C800_53_R3	Does the functional architecture define the unique security requirements?
1364	Organizational	C800_53_R3	Does the functional architecture define the types of information processed, stored, or transmitted by the system and any specific protection needs in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance?
1365	Organizational	C800_53_R3	Does the functional architecture define the restoration priority of information or system services?
1366	Organizational	C800_53_R3	Is a privacy impact assessment conducted on the system in accordance with Office of Management and Budget policy?
1367	Info Protection	C800_53_R3	Are the results of information security measures of performance monitored and reported?
1368	Organizational	C800_53_R3	Are individuals designated to fulfill specific roles and responsibilities within the organizational risk management process?
1369	Info Protection	C800_53_R3	Are information protection needs determined, and are the processes revised as necessary, until an achievable set is obtained?
1370	Personnel	C800_53_R3	Is every user accessing a system processing, storing, or transmitting classified information cleared and indoctrinated to the highest classification level of the information on the system?
1371	Personnel	C800_53_R3	Is every user accessing a system processing, storing, or transmitting types of classified information which require formal indoctrination, formally indoctrinated for all the relevant types of information on the system?
1372	Personnel	C800_53_R3	Is access to information with special protection measures granted only to individuals who have a valid access authorization that is demonstrated by assigned official government duties and that satisfy associated personnel security criteria?
1373	Personnel	C800_53_R3	Is access to classified information with special protection measures granted only to individuals who have a valid access authorization that is demonstrated by assigned official government duties?
1374	Personnel	C800_53_R3	Is access to classified information with special protection measures granted only to individuals that satisfy associated personnel security criteria consistent with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance?
1375	Personnel	C800_53_R3	Is access to classified information with special protection measures granted only to individuals that have read, understand, and signed a nondisclosure agreement?

1376	Monitoring & Malware	C800_53_R3	Are historic audit logs reviewed to determine if a vulnerability identified in the system has been previously exploited?
1377	System and Services Acquisition	C800_53_R3	Are software vendors/manufacturers required to demonstrate that their software development processes employ state-of-the-practice software and security engineering methods, quality control processes, and validation techniques to minimize flawed or malformed software?
1378	System and Services Acquisition	C800_53_R3	Is each system component acquired explicitly assigned to a system, and does the owner of the system acknowledge the assignment?
1379	System and Services Acquisition	C800_53_R3	Are system components required to be delivered in a secure documented configuration, and is the secure configuration the default configuration for any software reinstalls or upgrades?
1380	System and Services Acquisition	C800_53_R3	Are only government off-the-shelf or commercial off-the-shelf information assurance (IA) and IA-enabled information technology products employed that composes an NSA-approved solution to protect classified information when the networks used to transmit the information at a lower classification level than the information being transmitted?
1381	System and Services Acquisition	C800_53_R3	Have these products been evaluated and/or validated by the NSA or in accordance with NSA-approved procedures?
1382	System and Services Acquisition	C800_53_R3	Is the use of commercially provided information technology products limited to those products that have been successfully evaluated against a validated U.S. Government Protection Profile for a specific technology type?
1383	System and Services Acquisition	C800_53_R3	Is it required that the cryptographic module be FIPS-validated if no U.S. Government Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy?
1384	Information and Document Management	C800_53_R3	Are attempts to obtain system documentation documented when such documentation is either unavailable or nonexistent?
1385	Information and Document Management	C800_53_R3	Is the source code for the system protected and made available to authorized personnel?
1386	Information and Document Management	C800_53_R3	Is the use of binary or machine executable code prohibited from sources with limited or no warranty without accompanying source code?

1387	Information and Document Management	C800_53_R3	Are exceptions to the source code requirement provided only for compelling mission/operational requirements when no alternative solutions are available and with the express written consent of the authorizing official?
1388	System and Services Acquisition	C800_53_R3	Is an organizational assessment of risk conducted prior to the acquisition or outsourcing of dedicated information security services?
1389	System and Services Acquisition	C800_53_R3	Is the acquisition or outsourcing of dedicated information security services approved by a senior organizational official?
1390	System Protection	C800_53_R3	Is there a defined list of untrusted critical information system components that require re-implementation?
1391	System Protection	C800_53_R3	Are these untrusted information system components re-implemented or custom developed?
1392	System Protection	C800_53_R3	Is user functionality separated from system management functionality?
1393	System Protection	C800_53_R3	Is the presentation of system management-related functionality prevented at an interface for general users?
1394	System Protection	C800_53_R3	Are underlying hardware separation mechanisms used to facilitate security function isolation?
1395	Communication Protection	C800_53_R3	Is the discovery of specific system components (or devices) composing a managed interface prevented?
1396	Communication Protection	C800_53_R3	Are automated mechanisms used to enforce strict adherence to protocol format?
1397	Communication Protection	C800_53_R3	Are symmetric cryptographic keys using either NIST-approved or NSA-approved key management technology and processes produced, controlled, and distributed?
1398	Communication Protection	C800_53_R3	Are symmetric and asymmetric cryptographic keys using NSA-approved key management technology and processes produced, controlled, and distributed?
1399	Communication Protection	C800_53_R3	Are asymmetric cryptographic keys using approved PKI Class 3 certificates or prepositioned keying material produced, controlled, and distributed?
1400	Communication Protection	C800_53_R3	Are asymmetric cryptographic keys using approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key produced, controlled, and distributed?
1401	Communication Protection	C800_53_R3	Is FIPS-validated cryptography used to protect unclassified information?
1402	Communication Protection	C800_53_R3	Is NSA-approved cryptography used to protect classified information?

1403	Communication Protection	C800_53_R3	Is FIPS-validated cryptography used to protect information that must be separated from individuals who have the necessary clearances but lack the necessary access approvals?
1404	Communication Protection	C800_53_R3	Is either FIPS-validated or NSA-approved cryptography used to implement digital signatures?
1405	Portable/Mobile/Wireless	C800_53_R3	Does the acquisition, development, and/or use of mobile code to be deployed in the system meet defined mobile code requirements?
1406	Portable/Mobile/Wireless	C800_53_R3	Is the download and execution of prohibited mobile code prevented?
1407	Portable/Mobile/Wireless	C800_53_R3	Is the automatic execution of mobile code prevented in defined software applications, and are defined actions required prior to executing the code?
1408	Communication Protection	C800_53_R3	Are session identifiers invalidated upon user logout or other session termination?
1409	Communication Protection	C800_53_R3	Is a readily observable logout capability provided whenever authentication is used to gain access to Web pages?
1410	Communication Protection	C800_53_R3	Is a unique session identifier generated for each session, and are only system-generated session identifiers recognized?
1411	Communication Protection	C800_53_R3	Are unique session identifiers generated with defined randomness requirements?
1412	Monitoring & Malware	C800_53_R3	Are malicious code protection mechanisms tested on a defined frequency by introducing a known benign, nonspreading test case into the system and verifying that both detection of the test case and associated incident reporting occur?
1413	Physical Security	C800_53_R3	Are the communications traffic/event patterns analyzed for the system?
1414	Physical Security	C800_53_R3	Are profiles that represent the common traffic patterns and/or events developed?
1415	Physical Security	C800_53_R3	Are the traffic/event profiles used in tuning the system-monitoring devices to reduce the number of false positives and negatives to a defined measure?
1416	Physical Security	C800_53_R3	Is a wireless intrusion detection system used to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the system?
1417	Physical Security	C800_53_R3	Is an intrusion detection system used to monitor wireless communications traffic as the traffic passes from wireless to wireline networks?
1418	Physical Security	C800_53_R3	Is information from monitoring tools correlated to achieve organizationwide situational awareness?
1419	Physical Security	C800_53_R3	Are the results from monitoring physical, cyber, and supply chain activities correlated to achieve integrated situational awareness?

1420	System Integrity	C800_53_R3	Is the result of security function verification reported to designated organizational officials with information security responsibilities?
1421	Personnel	C800_53_R3	Is an exit interview conducted upon termination of employment?
1831	Access Control	C800_53_R4	Does the system allow authorized users to create and maintain security controls?
1832	Access Control	C800_53_R4	Does the system allow security attributes to be transmitted between distributed system components?
1833	Access Control	C800_53_R4	Does the system use proven techniques or technology to protect security attributes?
1834	Access Control	C800_53_R4	Does the organization have a security attribute re-grading mechanism that has been validated?
1835	Access Control	C800_53_R4	Does the system have authorized personnel to modify the security attributes on objects or persons?
1836	Access Control	C800_53_R4	Does the system maintain security attributes with the information?
1837	Access Control	C800_53_R4	Does the system establish permitted security values in security attributes?
1838	Access Control	C800_53_R4	Does the system allow permitted security values for each security attribute?
1839	Portable/Mobile/Wireless	C800_53_R4	Is the use of unclassified mobile device internal or external modem prohibited in a classified environment?
1840	Portable/Mobile/Wireless	C800_53_R4	Does the organization employ full-device encryption or container encryption to protect the confidentiality and integrity of information on organization defined mobile devices?
1841	Portable/Mobile/Wireless	C800_53_R4	Does the organization disable accounts of users found to be posing significant risk?
1842	Portable/Mobile/Wireless	C800_53_R4	Does the organization only permit the use of shared/group accounts that meet organization-defined conditions for establishing shared/group accounts?
1843	Portable/Mobile/Wireless	C800_53_R4	Does the system have the capacity to terminate group account credentials if members leave the group?
1844	System Protection	C800_53_R4	Does the organization detect and protect against data mining?
1845	Access Control	C800_53_R4	Does the information system transmit authorizations in a secure manner between systems?
1846	Access Control	C800_53_R4	Does the information system enforce access control and ensure that user identity or processes from a user are not disclosed based on security levels?
1847	Monitoring & Malware	C800_53_R4	Does the information system implement a reference monitor process that checks for access control permissions and has properties such as tamperproof, is always executing, and has a small resource footprint?

1848	Access Control	C800_53_R4	Does the Discretionary Access Control (DAC) policy allow users to specify and control sharing by named individuals or groups of individuals, or by both?
1849	Access Control	C800_53_R4	Does the Discretionary Access Control (DAC) policy limit propagation of access right?
1850	Access Control	C800_53_R4	Does the Discretionary Access Control (DAC) policy include or exclude access to the granularity of a single user?
1851	Communication Protection	C800_53_R4	Does the system identify information flows by data type, specification, and usage when transferring information between different security domains?
1852	Communication Protection	C800_53_R4	Does the system enforce security policies regarding information on interconnected systems?
1853	Access Control	C800_53_R4	Does the system provide separate processing domains to enable finer-grained allocation of user privileges?
1854	Access Control	C800_53_R4	Does the system prevent software from executing at higher privilege levels than the user?
1855	Access Control	C800_53_R4	Does the system display upon successful logon relevant organization information in addition to date and time of last logon?
1857	Audit and Accountability	C800_53_R4	Does the system allow for changing the level of auditing to meet organizational requirements?
1858	Audit and Accountability	C800_53_R4	Are automated mechanisms used to determine if organizational information has been disclosed in an unauthorized manner?
1859	Audit and Accountability	C800_53_R4	Does the organization review social networking site information being monitored?
1860	Audit and Accountability	C800_53_R4	Does the organization monitor social networking sites for unauthorized disclosure of organizational information?
1861	Audit and Accountability	C800_53_R4	Does the organization maintain user identity of cross-organization audit information?
1862	Audit and Accountability	C800_53_R4	Does the organization share services with other organizations and coordinate audit information transmitted across organizational boundaries?
1863	Audit and Accountability	C800_53_R4	Does the information system contain a secondary authoritative time source located in a different place than the primary time source?
1865	Audit and Accountability	C800_53_R4	Does the information system back up audit records daily onto a different system?
1866	Audit and Accountability	C800_53_R4	Does the organization enforce dual authorization to change or delete audit information?

1867	Audit and Accountability	C800_53_R4	Does the organization authorize read-only access to audit information for administrators?
1869	Risk Management and Assessment	C800_53_R4	Is the direct connection of a classified national security system prohibited to an external network without a boundary protection device?
1870	Risk Management and Assessment	C800_53_R4	Does the organization use analysis techniques on continuous monitoring process data and modifies the monitoring based on the results?
1871	Risk Management and Assessment	C800_53_R4	Does the organization establish target areas for a continuous monitoring program?
1872	Risk Management and Assessment	C800_53_R4	Does the organization continuously monitor security targets they have established?
1873	Risk Management and Assessment	C800_53_R4	Does the organization do a review of security information generated by continuous monitoring program?
1874	Risk Management and Assessment	C800_53_R4	Does the organization have response actions to address results of a security review?
1875	Risk Management and Assessment	C800_53_R4	Does the organization do penetration testing on information system according to a testing plan and defined frequency?
1876	Risk Management and Assessment	C800_53_R4	Does the system perform security compliance checks before establishing an internal connection?
1877	Risk Management and Assessment	C800_53_R4	Does the organization authorize and document interconnection of company owned information system?
1878	Configuration Management	C800_53_R4	Does the organization have cryptographic mechanisms under configuration management?
1879	Configuration Management	C800_53_R4	Does the system prevent the installation of software without verification of digital signature that is recognized and approved?
1880	Configuration Management	C800_53_R4	Is there a defined list of software programs authorized to execute on the system? Is the authorization policy a deny-all, permit-by-exception for software allowed to execute on the system? Is it reviewed at least annually?
1881	Configuration Management	C800_53_R4	Does the organization store component information and send the component owner an acknowledgment of this assignment?
1882	Configuration Management	C800_53_R4	Does the organization implement a configuration management plan that addresses roles, responsibilities, and management process and procedures?
1883	Configuration Management	C800_53_R4	Does the organization protect the configuration management plan from unauthorized disclosure and modification?
1884	Software	C800_53_R4	Is open source software usage restricted based on company policy?

1885	Software	C800_53_R4	Does the organization enforce user software installation?
1886	Software	C800_53_R4	Does the organization monitor compliance of user installed software?
1887	Software	C800_53_R4	Does the system monitor and alert when users have installed unauthorized software?
1888	Software	C800_53_R4	Does the system prohibit users from installing software (e.g., least user privileges)?
1889	Continuity	C800_53_R4	Is there a formal, documented contingency planning policy for the information system that addresses essential missions, business functions, and full system restoration despite a system catastrophic failure. In addition, does the plan include restoration of security safeguards and is the plan reviewed and approved by key personnel?
1890	Continuity	C800_53_R4	Is the information system contingency plan reviewed according to company policy time period?
1891	Continuity	C800_53_R4	Is the information system contingency plan updated when changes occur in the company or system?
1892	Continuity	C800_53_R4	Is the modified information system contingency plan distributed to contingency personnel?
1893	Continuity	C800_53_R4	Is the information system contingency plan protected from unauthorized disclosure and modification?
1894	Continuity	C800_53_R4	Does the organization identify critical information system assets?
1895	Continuity	C800_53_R4	Does the organization have a contingency plan for resumption of company business functions within a company-defined time period?
1896	Continuity	C800_53_R4	Does the organization plan for recovery of essential missions and business functions reducing loss of operation and sustains continuity until full system restoration at the primary site?
1897	Continuity	C800_53_R4	Does the organization plan for transfer of essential missions and business functions to an alternate site with little loss of operational continuity?
1898	Continuity	C800_53_R4	Does the organization coordinate its contingency plan with external service providers to ensure contingency requirements can be satisfied?
1899	Training	C800_53_R4	Does the organization provide contingency training to system users of their contingency role and responsibility in recovery? Also when contingency plans change and are they done within a predetermined time allowance?
1900	Training	C800_53_R4	Does the organization use simulated events in contingency training to facilitate personnel response?
1901	Training	C800_53_R4	Does the organization use automated mechanisms to make contingency training more realistic?

1902	Training	C800_53_R4	Does the organization test the contingency plan on a company-defined time interval and frequency to determine the effectiveness of the plan?
1903	Training	C800_53_R4	Does the organization review the contingency plan test results and makes corrective action changes if needed?
1904	Training	C800_53_R4	Does the organization coordinate contingency plan testing with groups responsible for the design?
1905	Training	C800_53_R4	Does the organization test the continuity plan at the alternate processing site to gain familiarity and to evaluate capabilities with the site?
1906	Continuity	C800_53_R4	Does the alternate site have equipment required to transfer business operations and are contracts in place to support the transfer within a prescribed time frame?
1907	Continuity	C800_53_R4	Does the organization plan and prepare for situations where returning to normal operations from the primary site is prevented?
1908	Communication Protection	C800_53_R4	Does the organization request Telecommunications Service Priority for all telecommunication services used for national security emergency preparedness, especially when primary and secondary providers are the same?
1909	Communication Protection	C800_53_R4	Does the organization test alternate telecommunication services at least annually?
1910	Continuity	C800_53_R4	Does the organization enforce dual authorization for destruction of backup media containing data?
1911	Continuity	C800_53_R4	Does the organization protect backup and restoration hardware, firmware, and software?
1912	Continuity	C800_53_R4	Does the system provide alternate communication protocols in support of maintaining continuity of operations?
1913	Continuity	C800_53_R4	Does the system enter a safe mode with operation restrictions when abnormal conditions are detected?
1914	Continuity	C800_53_R4	Are there alternative security mechanisms available to provide system security when the primary security functions fail or are compromised?
1915	Access Control	C800_53_R4	Is multifactor authentication used for remote access to privileged accounts where one of the factors is provided by a device separate from the system being accessed?
1916	Access Control	C800_53_R4	Does the information system accept and electronically verify Personal Identity Verification credentials?
1917	Access Control	C800_53_R4	Does the organization require user authentication even though a group authenticator is available?

1918	Access Control	C800_53_R4	Is multifactor authentication used for network access to privileged accounts where one of the factors is provided by a device separate from the system being accessed?
1919	Access Control	C800_53_R4	Is single sign-on capability available on the system?
1920	Access Control	C800_53_R4	Does the organization have a process to ensure that device identification and authentication based on attestation is handled?
1921	Account Management	C800_53_R4	Are user or device identifiers disabled after a time period of inactivity (e.g., 30 days)?
1922	Account Management	C800_53_R4	Is the registration process to receive a user authenticator carried out in person before a designated registration authority and require supervisor authorization?
1923	Audit and Accountability	C800_53_R4	Does the organization coordinate with external organizations for cross-organization management of identifiers?
1924	Access Control	C800_53_R4	When changes to group accounts occur are password changes made as well?
1925	Access Control	C800_53_R4	Do hardware token-based authentication devices satisfy quality requirements?
1926	Access Control	C800_53_R4	Does the registration process require authenticators to be given in person by authorized personnel?
1927	Access Control	C800_53_R4	Does the organization protect authenticators at the same level of security as the information?
1928	Access Control	C800_53_R4	Are external organizations required to coordinate credentials?
1929	Access Control	C800_53_R4	Does the system dynamically provision identities (e.g., for smart card binding)?
1930	Access Control	C800_53_R4	Does the system prohibit the use of cached authenticators after a specified time?
1931	Access Control	C800_53_R4	Does the organization employ an organization-wide methodology for managing the content of PKI trusted stores installed across all platforms including networks, operating systems, browsers, and applications?
1932	Access Control	C800_53_R4	Does the organization use only FICAM approved path discovery and validation products and services?
1933	Access Control	C800_53_R4	Does the system accept FICAM-approved credentials?
1934	Access Control	C800_53_R4	Does the organization employ only FICAM-approved information system components to accept third-party credentials?
1935	Access Control	C800_53_R4	Does the system conform to FICAM-issued profiles?
1936	Access Control	C800_53_R4	Does the system accept and verifies PIV-I credentials?
1937	Access Control	C800_53_R4	Does the organization ensure that service providers receive, validate, and transmit identification and authentication information?
1938	Access Control	C800_53_R4	Does accessing the system under special circumstances still require authentication?

1939	Access Control	C800_53_R4	Does the user re-authenticate when circumstances require (e.g., when authenticators or roles change, after time out)?
1940	Incident Response	C800_53_R4	Are there incident handling capabilities for insider threats?
1941	Incident Response	C800_53_R4	Are there coordinated incident handling capabilities for insider threats across the organization?
1942	Incident Response	C800_53_R4	Do external organizations coordinate with and correlate shared incident information to achieve a cross-organizational incident awareness and effective incident response?
1943	Incident Response	C800_53_R4	Does the organization use dynamic responses when responding to security incidences?
1944	Incident Response	C800_53_R4	Does the organization coordinate incident handling activities which involve vendor supply chain activities with other organizations involved in the supply chain?
1946	Incident Response	C800_53_R4	Does the organization report security incident information to vendors of the system?
1947	Incident Response	C800_53_R4	Is the incident response plan protected from unauthorized disclosure and modification?
1948	Incident Response	C800_53_R4	Does the organization have a plan to respond to information spills that is comprehensive?
1949	Incident Response	C800_53_R4	Are there personnel identified and responsible for responding to information spills?
1950	Incident Response	C800_53_R4	Does the organization provide information spillage response training on a defined frequency?
1951	Incident Response	C800_53_R4	Does the organization have procedures that ensure continuity while the information spill is active and undergoing corrective actions?
1952	Incident Response	C800_53_R4	Does the organization inform personnel of responsibility associated with exposure to information spillage?
1953	Incident Response	C800_53_R4	Does the organization have an integrated team of forensic analysts, tool developers, and real-time personnel established?
1954	Maintenance	C800_53_R4	Is predictive maintenance used in your organization?
1955	Maintenance	C800_53_R4	Does the organization employ automated mechanisms to transfer predictive maintenance data to a computerized maintenance management system?
1956	Info Protection	C800_53_R4	Does the organization restrict the use of system media that can't be sanitized?
1957	Info Protection	C800_53_R4	Does the organization have an erasing process for digital media that is established according to procedures?
1958	Info Protection	C800_53_R4	Does the organization document the erase system media process?

1959	Info Protection	C800_53_R4	Does the organization employs tests of media erasing equipment and procedures to verify correct performance regularly?
1960	Info Protection	C800_53_R4	Does the organization erase information system media, containing Controlled Unclassified Information (CUI) prior to public release in accordance with applicable federal and organizational standards and policies?
1961	Info Protection	C800_53_R4	Does the organization erase information system media, containing classified information prior to release to individuals without required access authorizations in accordance with NSA standards and policies?
1962	Access Control	C800_53_R4	Does the organization control physical access to output devices (displays, printers) and ensure only authorized users receive output from the device?
1963	Access Control	C800_53_R4	Do you control physical access and verify identity of the person receiving the output from the device (e.g., pin or hardware tokens)?
1964	Access Control	C800_53_R4	Does the organization mark system output devices with the appropriate security marking of the information permitted to be output from the device?
1965	Access Control	C800_53_R4	Does the organization employ automated mechanisms to recognize classes/types of intrusions and initiate response actions?
1966	Access Control	C800_53_R4	Does the organization employ video surveillance of operational areas and retain video recordings for a specified time period?
1967	Physical Security	C800_53_R4	Does the organization employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source?
1968	Incident Response	C800_53_R4	Does the organization implement an insider threat program that includes a cross-discipline insider threat incident handling team?
1969	Organizational	C800_53_R4	Does the organization establish an information security workforce development and improvement program?
1970	Organizational	C800_53_R4	Does the organization have a process for conducting security testing, training, and monitoring which are maintained and executed in a timely manner? Also, are periodic reviews done on these plans for consistency and according to company policy?
1971	Organizational	C800_53_R4	Does the organization maintain contact with selected security groups to facilitate training on current security practices, share security-related information?
1972	Organizational	C800_53_R4	Does the organization implement a threat awareness program that includes a cross-organization information-sharing capability?

1973	Personnel	C800_53_R4	Does the organization notify terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information?
1974	Risk Management and Assessment	C800_53_R4	Does the organization update the information system vulnerabilities list when new vulnerabilities are identified and reported?
1975	Risk Management and Assessment	C800_53_R4	Does the system implement privileged access authorization to system components for selected vulnerability scanning activities?
1976	Risk Management and Assessment	C800_53_R4	Does the organization correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors?
1977	Risk Management and Assessment	C800_53_R4	Does the organization employ a technical surveillance countermeasure survey at least once a year?
1978	System and Services Acquisition	C800_53_R4	Does the organization restrict the location of information processing based on requirements or conditions?
1979	System and Services Acquisition	C800_53_R4	Does the organization approve, document, and control the use of live data in development and test environments for the system, system component, or system service?
1980	System and Services Acquisition	C800_53_R4	Does the organization require the developer of the system to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security review?
1981	System and Services Acquisition	C800_53_R4	Does the organization require the developer of the system to provide training on the correct use and operation of the implemented security functions, controls, and/or mechanisms?
1982	System and Services Acquisition	C800_53_R4	Does the organization require the developers of the system, system components, or system services to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege principles?
1983	System and Services Acquisition	C800_53_R4	Does the organization train personnel to detect counterfeit information system components (including hardware, software, and firmware)?
1984	System and Services Acquisition	C800_53_R4	Does the organization require that developers of the system are trustworthy and are able to pass a personnel screening test?
1985	System and Services Acquisition	C800_53_R4	Does the organization ensure that steps have been taken to verify the personnel screening of those who performed work on the system?
1986	Communication Protection	C800_53_R4	Does the organization employ monitoring tools to detect indicators of denial of service attacks against the information system and monitors system resources to determine if sufficient resources exist to prevent effective denial-of-service attacks?

1987	Communication Protection	C800_53_R4	Does the organization allow execution of permitted mobile code only in confined virtual machine environments?
1988	Communication Protection	C800_53_R4	Does the organization remove from online storage and stores off-line in a secure location system information?
1989	Communication Protection	C800_53_R4	Does the organization employ realistic, but misleading information in the system with regard to its security state or posture?
1990	Communication Protection	C800_53_R4	Does the organization employ techniques to hide or conceal information system components?
1991	Communication Protection	C800_53_R4	Does the organization measure the bandwidth of a subset of identified covert channels in the operational environment of the information system?
1992	Communication Protection	C800_53_R4	Does the organization distribute processing and storage across multiple physical locations?
1993	Communication Protection	C800_53_R4	Does the organization employ polling techniques to identify potential faults, errors, or compromises to distributed processing and storage components?
1994	Communication Protection	C800_53_R4	Does the organization employ out-of-band channels for the physical delivery or electronic transmission of information, information system components, or devices to individuals or information systems?
1995	Communication Protection	C800_53_R4	Does the information system maintain a separate execution domain for each executing process?
1996	Communication Protection	C800_53_R4	Does the information system maintain a separate execution domain for each thread in multi-threaded processing?
1997	Communication Protection	C800_53_R4	Does the information system implement cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters?
1998	Communication Protection	C800_53_R4	Does the information system implement cryptographic mechanisms to prevent the identification of wireless transmitters by using the transmitter signal parameters?
1999	Communication Protection	C800_53_R4	Does the information system prohibit the remote activation of environmental sensing capabilities except where remote activation of sensors is allowed and provides an explicit indication of sensor use?
2000	Communication Protection	C800_53_R4	Does the organization ensure that the system is configured so that data or information collected by the sensors is only reported to authorized individuals or roles?
2001	Communication Protection	C800_53_R4	Does the organization use data or information collected only for authorized purposes?

2002	Communication Protection	C800_53_R4	Does the organization establishes usage restrictions and implementation guidance for system components based on the potential to cause damage to the information system if used maliciously? And does the organization authorize, monitor, and control the use of such components within the information system?
2003	System Integrity	C800_53_R4	Does the organization remove software and firmware components after updated versions have been installed?
2004	System Integrity	C800_53_R4	Does the information system implement nonsignature-based malicious code detection mechanisms?
2005	System Integrity	C800_53_R4	Does the organization implement additional monitoring of individuals who have been identified by sources as posing an increased level of risk?
2006	System Integrity	C800_53_R4	Does the organization implement additional monitoring of privileged users?
2007	System Integrity	C800_53_R4	Does the system automatically shut down when integrity violations are discovered?
2008	System Integrity	C800_53_R4	Does the system verify the integrity of the boot process of devices?
2009	System Integrity	C800_53_R4	Does the organization require that user-installed software execute in a confined physical or virtual machine environment with limited privileges?
2010	System Integrity	C800_53_R4	Does the organization requires that the integrity of user-installed software be verified prior to execution?
2011	System Integrity	C800_53_R4	Does the organization allow execution of binary or machine-executable code obtained from sources with limited or no warranty and without the provision of source code only in confined physical or virtual machine environments and with explicit approval?
2012	System Integrity	C800_53_R4	Does the organization prohibit the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code and provide exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official?
2013	System Integrity	C800_53_R4	The information system implements cryptographic mechanisms to authenticate software or firmware components prior to installation?
2014	System Integrity	C800_53_R4	Does the information system implement cryptographic mechanisms to authenticate software or firmware components prior to installation?
2015	System Integrity	C800_53_R4	Does the information system implement spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic?
2016	System Integrity	C800_53_R4	Does the organization ensure that input validation errors are reviewed and resolved within defined time period?

2017	System Integrity	C800_53_R4	Does the information system behave in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received?
2018	System Integrity	C800_53_R4	Does the organization account for timing interactions among information system components in determining appropriate responses for invalid inputs?
2019	System Integrity	C800_53_R4	Does the organization restrict the use of information inputs to trusted sources and/or formats?
2020	System Integrity	C800_53_R4	Does the organization provide real-time failover capability for the system?
2021	System Integrity	C800_53_R4	Does the organization implement non-persistent information system components and services?
2022	System Integrity	C800_53_R4	Does the information system implement security safeguards to protect its memory from unauthorized code execution?
2025	Access Control	C800_53_R4	Does the information system have out-of-band authentication designed for use under abnormal condition?
2026	Physical Security	C800_53_R4	Does the organization employ automatic voltage controls for critical information system components?
2028	Access Control	C800_53_R4	Are access privileges to protected information reviewed at least annually to confirm they are correct and that they correspond to the organizations' needs and appropriate personnel roles and responsibilities?
2801	Privacy	C800_53_R4_App_J	Does the organization determine and document the legal authority that permits the collection, use, maintenance, and sharing of PII, in general or in support of a specific program or information system need?
2802	Privacy	C800_53_R4_App_J	Does the organization document the purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices?
2803	Privacy	C800_53_R4_App_J	Does the organization appoint a Senior Agency Official for Privacy (SAOP) and a Chief Privacy Officer (CPO) who are accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information system?
2804	Privacy	C800_53_R4_App_J	Does the organization monitor federal privacy laws and policy for changes that affect the privacy program?
2805	Privacy	C800_53_R4_App_J	Does the organization allocate appropriate level of funding and resources to implement and operate the organization-wide privacy program?
2806	Privacy	C800_53_R4_App_J	Does the organization develop a privacy plan for implementing applicable privacy controls, policies, and procedures?

2807	Privacy	C800_53_R4_App_J	Does the organization develop, disseminate, and implement operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII?
2808	Privacy	C800_53_R4_App_J	Does the organization update the privacy plan, policies, and procedures according to company-defined time period or at least biennially?
2809	Privacy	C800_53_R4_App_J	Does the organization document and implement a privacy risk management process that assesses privacy risk to individuals resulting from collection, sharing, storing, transmitting, use, or disposal of PII?
2810	Privacy	C800_53_R4_App_J	Does the organization conduct Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures?
2811	Privacy	C800_53_R4_App_J	Does the organization establish privacy roles, responsibilities, and access requirements for contractors and service providers?
2812	Privacy	C800_53_R4_App_J	Does the organization include privacy requirements in contracts and other acquisition-related documents?
2813	Privacy	C800_53_R4_App_J	Does the organization monitor and audit privacy controls and internal privacy policy according to company-defined time interval to ensure effective implementation?
2814	Privacy	C800_53_R4_App_J	Does the organization develop, implement, and update comprehensive training and awareness for ensuring personnel understand privacy responsibilities and procedures?
2815	Privacy	C800_53_R4_App_J	Does the organization administer basic privacy training at least annually and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII, and is this done at least annually?
2816	Privacy	C800_53_R4_App_J	Does the organization ensure that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements at least annually?
2817	Privacy	C800_53_R4_App_J	Does the organization develop, distribute, and update reports to OMB, Congress, and other oversight bodies to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance?
2818	Privacy	C800_53_R4_App_J	Does the organization design information systems to support privacy by automating privacy controls?

2819	Privacy	C800_53_R4_App_J	Does the organization keep an accurate accounting of disclosures of information held in each system of records under its control that includes the Date, nature, and purpose of each disclosure of a record and name with the address of the person or agency to which the disclosure was made?
2820	Privacy	C800_53_R4_App_J	Does the organization retain the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer?
2821	Privacy	C800_53_R4_App_J	Does the organization make the accounting of disclosures available to the person named in the record upon request?
2822	Privacy	C800_53_R4_App_J	Does the organization confirm upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information?
2823	Privacy	C800_53_R4_App_J	Does the organization collect PII directly from the individual to the greatest extent practical?
2824	Privacy	C800_53_R4_App_J	Does the organization check for, and correct, as necessary, any inaccurate or outdated PII used by its programs or systems?
2825	Privacy	C800_53_R4_App_J	Does the organization issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information?
2826	Privacy	C800_53_R4_App_J	Does the organization request that the individual or individual's authorized representative validate PII during the collection process?
2827	Privacy	C800_53_R4_App_J	Does the organization request that the individual or individual's authorized representative revalidate that PII collected is still accurate according to company policy?
2828	Privacy	C800_53_R4_App_J	Does the organization document processes to ensure the integrity of PII through existing security controls?
2829	Privacy	C800_53_R4_App_J	Does the organization establish a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act?
2830	Privacy	C800_53_R4_App_J	Does the organization publish Computer Matching Agreements on its public Web site?
2831	Privacy	C800_53_R4_App_J	Does the organization identify the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection?
2832	Privacy	C800_53_R4_App_J	Does the organization limit the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent?

2833	Privacy	C800_53_R4_App_J	Does the organization conduct an initial evaluation of PII holdings and establish and follow a schedule for regularly reviewing those holdings at least annually to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose?
2834	Privacy	C800_53_R4_App_J	Does the organization locate and remove or redact specified PII and/or uses anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure?
2835	Privacy	C800_53_R4_App_J	Does the organization retain each collection of PII for company defined time period to fulfill the purpose(s) identified in the notice or as required by law?
2836	Privacy	C800_53_R4_App_J	Does the organization dispose of, destroy, erase, and/or anonymize the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access?
2837	Privacy	C800_53_R4_App_J	Does the organization use company-defined techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records)?
2838	Privacy	C800_53_R4_App_J	Does the organization configure its information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule?
2839	Privacy	C800_53_R4_App_J	Does the organization develop policies and procedures that minimize the use of PII for testing, training, and research?
2840	Privacy	C800_53_R4_App_J	Does the organization implement controls to protect PII used for testing, training, and research?
2841	Privacy	C800_53_R4_App_J	Does the organization use techniques to minimize the risk to privacy of using PII for research, testing, or training?
2842	Privacy	C800_53_R4_App_J	Does the organization provide means for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection?
2843	Privacy	C800_53_R4_App_J	Does the organization provide appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII?
2844	Privacy	C800_53_R4_App_J	Does the organization obtain consent from individuals prior to any new uses or disclosure of previously collected PII?

2845	Privacy	C800_53_R4_App_J	Does the organization ensure that individuals are aware of and consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII?
2846	Privacy	C800_53_R4_App_J	Does the organization implement mechanisms to support itemized or tiered consent for specific uses of data?
2847	Privacy	C800_53_R4_App_J	Does the organization provide individuals the ability to have access to their PII maintained in its systems of records?
2848	Privacy	C800_53_R4_App_J	Does the organization publish rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records?
2849	Privacy	C800_53_R4_App_J	Does the organization publish access procedures in System of Records Notices (SORNs)?
2850	Privacy	C800_53_R4_App_J	Does the organization adhere to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests?
2851	Privacy	C800_53_R4_App_J	Does the organization provide a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate?
2852	Privacy	C800_53_R4_App_J	Does the organization have an established process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and notifies affected individuals that their information has been corrected or amended?
2853	Privacy	C800_53_R4_App_J	Does the organization implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices?
2854	Privacy	C800_53_R4_App_J	Does the organization respond to complaints, concerns, or questions from individuals within the company defined time period?
2855	Privacy	C800_53_R4_App_J	Does the organization establish, maintain, and update according to company policy, an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII?
2856	Privacy	C800_53_R4_App_J	Does the organization provide each update of the PII inventory to the CIO or information security official, according to company time intervals, to support the establishment of information security requirements for all new or modified information systems containing PII?
2857	Privacy	C800_53_R4_App_J	Does the organization develop and implement a Privacy Incident Response Plan?

2858	Privacy	C800_53_R4_App_J	Does the organization provide an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan?
2859	Privacy	C800_53_R4_App_J	Does the organization provide effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII; (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary?
2860	Privacy	C800_53_R4_App_J	Does the organization describe: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected?
2861	Privacy	C800_53_R4_App_J	Does the organization revise its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or soon after the change?
2862	Privacy	C800_53_R4_App_J	Does the organization provide real-time and/or a layered notice when it collects PII?
2863	Privacy	C800_53_R4_App_J	Does the organization publish System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing PII?
2864	Privacy	C800_53_R4_App_J	Does the organization keep System of Records Notices (SORNs) current?
2865	Privacy	C800_53_R4_App_J	Does the organization include Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected?
2866	Privacy	C800_53_R4_App_J	Does the organization publish System of Records Notices (SORNs) on its public website?
2867	Privacy	C800_53_R4_App_J	Does the organization ensure that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)?
2868	Privacy	C800_53_R4_App_J	Does the organization ensure that its privacy practices are publicly available through organizational websites or otherwise?

2869	Privacy	C800_53_R4_App_J	Does the organization use PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices?
2870	Privacy	C800_53_R4_App_J	Does the organization share PII externally, only for the authorized purposes identified in the Privacy Act and/or described in its notices or for a purpose that is compatible with those purposes?
2871	Privacy	C800_53_R4_App_J	Does the organization enter into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used?
2872	Privacy	C800_53_R4_App_J	Does the organization monitor, audit, and train its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII?
2873	Privacy	C800_53_R4_App_J	Does the organization evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required?
1422	Organizational	C800_82	Is there a cross-functional cybersecurity team consisting of ICS personnel, IT personnel, and system vendors/system integrators that reports to and is accountable to management?
1423	Organizational	C800_82	Does the cybersecurity team consist of a member from the IT staff, a control engineer, a control system operator, a security subject matter expert, and a member of management?
1424	Organizational	C800_82	Does the cross-functional cybersecurity team, include network architecture and design personnel, security processes and practices personnel, and secure infrastructure design and operation personnel?
1425	Organizational	C800_82	Does the cybersecurity team have a charter defining the roles, responsibilities, and accountabilities?
1426	Organizational	C800_82	Does the cybersecurity team report directly to site management or the company's CIO/CSO, who in turn, accepts complete responsibility and accountability for the cybersecurity of the system?
1427	Policies & Procedures General	C800_82	Is the physical security organization aware of the locations of sensitive equipment?
1428	Plans	C800_82	Are interruptions to the recovery process defined and procedures in place to handle them?
1429	System Protection	C800_82	Are external incidents reviewed to determine if they are applicable?

1430	Communication Protection	C800_82	Are critical networks redundant?
1431	Training	C800_82	Does the awareness and training program cover the physical process being controlled?
1432	Plans	C800_82	Does the disaster recovery plan include procedures for operating the system in manual mode until secure conditions are restored?
1433	Plans	C800_82	Does the disaster recovery plan include a complete and up-to-date logical network diagram?
1434	Plans	C800_82	Does the disaster recovery plan include a communication procedure and list of personnel to contact in the case of an emergency?
1435	Plans	C800_82	Does the disaster recovery plan include the requirements for the timely replacement of components in the case of an emergency?
1436	Continuity	C800_82	Are critical replacements for hard-to-obtain components kept in inventory?
1437	Plans	C800_82	Does the contingency plan cover the full range of failures and problems caused by cyber incidents?
1438	Plans	C800_82	Are the business continuity and disaster recovery plans closely related to the contingency plans?
1439	System Integrity	C800_82	Are the security controls present during system validation testing, and are they still installed and operating correctly in the production system?
1440	System Integrity	C800_82	Is the production system free from security compromises, and does it provide information on the nature and extent of compromises, should they occur?
1441	Monitoring & Malware	C800_82	Are the system performance metrics sent to appropriate stakeholders?
1442	Monitoring & Malware	C800_82	Are system auditing utilities incorporated into new and existing projects?
1443	Monitoring & Malware	C800_82	Are auditing utilities tested offline before being deployed on an operational system?
1444	System Integrity	C800_82	Is there an active test facility that replicates the existing system to a high degree, and are changes tested on the test system before being deployed on the main system?
1445	System Integrity	C800_82	Is the system software regression tested to ensure that it meets the security requirements of the current installation?
1446	System Integrity	C800_82	Are the built-in security capabilities of software and components used?
1447	System Integrity	C800_82	Are patches applied during planned ICS maintenance cycles?
1448	System Integrity	C800_82	Are there procedures to guide patch deployment testing and installation?

1449	System Integrity	C800_82	Is OPC updated with patches to handle RPC/DCOM vulnerabilities?
1450	System Protection	C800_82	Have single points of failure been evaluated when securing the network, and has a risk assessment been performed to remediate those points found problematic?
1451	System Protection	C800_82	Are critical components redundant to prevent single point failures?
1452	Environmental Security	C800_82	Are components and systems shielded from RF signals?
1453	Environmental Security	C800_82	Are unshielded twisted pair cables prohibited?
1454	Environmental Security	C800_82	Are industrial RJ-45 connectors used for twisted pair connectors?
1455	Environmental Security	C800_82	Are fiber optic and/or coax cables used to eliminate interference?
1456	Environmental Security	C800_82	Are cables and connectors color coded and labeled to prevent cross connections?
1457	Environmental Security	C800_82	Are cable runs installed to prevent unintended access?
1458	Environmental Security	C800_82	Is equipment installed in locked cabinets with proper ventilation and air filtration?
1459	Physical Security	C800_82	Is a ringed layer of defense used for access to the facility?
1460	Account Management	C800_82	Does access control take into account the special needs of personnel to access equipment and perform their job duties?
1461	Access Control	C800_82	Do passwords avoid predictable sequences of numbers, are not found in dictionaries, and meet strength requirements?
1462	Access Control	C800_82	Is the passwords administrator a trusted employee who is available during emergencies and are copies of passwords stored securely?
1463	Access Control	C800_82	Are the privileged user passwords more secure and changed frequently?
1464	Access Control	C800_82	Is the authority to change master passwords limited to a trusted employee?
1465	Access Control	C800_82	Is a password audit record, especially for master passwords, maintained separately from the system?
1466	Access Control	C800_82	Are network device passwords changed on a regular basis?
1467	Access Control	C800_82	Are passwords used on system components and are they implemented to not interfere with emergency actions?

1468	Access Control	C800_82	Is PIV (Personal Identity Verification) used and does it conform to the requirements of FIPS 201 and NIST SP 800-73 and employ either cryptographic verification or biometric verification?
1469	Access Control	C800_82	Is token-based access control with cryptographic verification used, and does it conform to the requirements of NIST SP 800-78?
1470	Access Control	C800_82	Is token-based access control that employs biometric verification used, and does it conform to the requirements of NIST SP 800-76?
1471	Access Control	C800_82	Is challenge/response authentication used whenever possible and practical?
1472	Account Management	C800_82	Is biometric authentication used where it is most appropriate and are the issues associated with biometric authentication understood?
1473	Communication Protection	C800_82	Is HTTPS used instead of HTTP, and SFTP, or SCP instead of FTP for Web services on control devices?
1474	Communication Protection	C800_82	Is inbound FTP and email traffic blocked for control devices?
1475	Monitoring & Malware	C800_82	Has the use of antivirus software on devices with real time dependent code been evaluated and does the vendor support installation of antivirus code?
1476	Monitoring & Malware	C800_82	Is malware protection software and definitions reviewed and thoroughly tested?
1477	Communication Protection	C800_82	Are data flow controls tested to ensure they do not adversely impact the system?
1478	Maintenance	C800_82	Are devices used for programming or maintenance/administrative functions secured in the system environment?
1479	Portable/Mobile/Wireless	C800_82	Are laptops, portable engineering workstations, handhelds, and specialized devices secured in the system environment?
1480	Communication Protection	C800_82	Are multiple DMZs and intrusion detection systems used that apply different rule-sets to each unique domain being monitored?
1481	Communication Protection	C800_82	Are network-based IDS/IPS capabilities deployed between the control network and corporate network with a firewall?
1482	Communication Protection	C800_82	Are host-based IDS/IPS capabilities used on appropriate devices?
1483	Communication Protection	C800_82	Is control system traffic given priority over any noncontrol system traffic?

1484	Communication Protection	C800_82	Is the system configured so IT network services provide maximum priority to all control system traffic, and is the network analyzed to ensure control system traffic is not dependent on IT network services (i.e., DNS services)?
1485	Communication Protection	C800_82	Is network traffic secured from protocol analyzers and other utilities that could use the information to craft traffic to manipulate system activity?
1486	Communication Protection	C800_82	Is a properly configured DMZ or a VPN connection used between the control system and the corporate network?
1487	Communication Protection	C800_82	Are security servers placed directly in the DMZ (e.g., patch management, anti-virus, IDS, etc.)?
1488	Communication Protection	C800_82	Are the risks of a DMZ fully understood?
1489	Communication Protection	C800_82	Is a DMZ with paired firewalls (from different vendors) deployed between the corporate and control system networks?
1490	Communication Protection	C800_82	Is a three-zone system used with two historians - one on the control system side synced with one in the DMZ?
1491	Communication Protection	C800_82	Are methods employed for handling packets that are undefined, poorly defined, or contain unexpected field values?
1492	Communication Protection	C800_82	Are passwords and device configurations secured when transmitted across media that are susceptible to eavesdropping?
1493	Communication Protection	C800_82	Is the use of vulnerability scanners prohibited or are they only used on test or insensitive redundant systems?
1494	Monitoring & Malware	C800_82	Are network protocol integrity checks built-in or provided by other techniques for control system traffic?
1495	Communication Protection	C800_82	Are Faraday cages or other devices used to limit the wireless signal as required?
1496	Portable/Mobile/Wireless	C800_82	Are wireless users authenticated using IEEE 802.1X that authenticates users via certificates or RADIUS servers?
1497	Portable/Mobile/Wireless	C800_82	Are wireless services located on a dedicated and isolated server with minimal connections to the system network?
1498	Portable/Mobile/Wireless	C800_82	Are wireless access points configured to have a unique service set identifier (SSID), disabled SSID broadcast, and enabled MAC filtering?
1499	Portable/Mobile/Wireless	C800_82	Are wireless devices configured into a separate organizational unit of the Windows domain? (For a Microsoft Windows network)

1500	Portable/Mobile/Wireless	C800_82	Is encryption done at OSI Layer 2 (data layer) to reduce latency?
1501	Portable/Mobile/Wireless	C800_82	Are hardware accelerators used for encryption to reduce latency?
1502	Portable/Mobile/Wireless	C800_82	Are DNS requests out of the control network prohibited and are DNS requests from the control network to the DMZ reviewed and approved?
1503	Communication Protection	C800_82	Is HTTP prevented from crossing network boundaries?
1504	Communication Protection	C800_82	Do HTTP proxies block all inbound scripts and Java applications?
1505	Communication Protection	C800_82	Is HTTPS implemented if HTTP is required?
1506	Communication Protection	C800_82	Are all TFTP sessions blocked?
1507	Communication Protection	C800_82	Is FTP used when it is authenticated with a multifactor passcode and encrypted in a tunnel?
1508	Communication Protection	C800_82	Are secure FTP and secure copy employed whenever possible?
1509	Communication Protection	C800_82	Is telnet prohibited or only used inbound from the corporate network with a token-based multifactor password and encrypted tunnel?
1510	Communication Protection	C800_82	Are outbound telnet sessions allowed only over encrypted tunnels to specific devices?
1511	Communication Protection	C800_82	Is SMTP not used for inbound mail and only used for outbound alert messages?
1512	Communication Protection	C800_82	Is SNMP V1 or V2 used over a secured management network or is SNMP V3 used with the security features built-in?
1513	Communication Protection	C800_82	Is the DCOM protocol used only between the control network and the DMZ networks and is the protocol between the DMZ and the corporate network explicitly blocked?
1514	Communication Protection	C800_82	Are DCOM port ranges restricted by making registry modifications on devices using DCOM?
1515	Communication Protection	C800_82	Is MODBUS/TCP, Ethernet/IP or DNP317 only used within the control network and explicitly not allowed on the corporate network?
1516	Communication Protection	C800_82	Is the use of NAT carefully reviewed before deployment?

1517	Communication Protection	C800_82	Are multicast protocols with IGMP used when using multiple LANs?
1518	Communication Protection	C800_82	Are "loss of communications" and the appropriate fail-safe process defined?
1519	Communication Protection	C800_82	Is an appropriate fail-safe process executed upon the loss of communications?
1520	Communication Protection	C800_82	Is MAC address locking implemented to prevent man-in-the-middle attacks?
1521	Communication Protection	C800_82	Are statically coded ARP tables implemented on capable devices?
1522	Communication Protection	C800_82	Is the system monitored for ARP poisoning? (i.e., corrupting host tables.)
1523	Communication Protection	C800_82	Are VLANs effectively deployed, with each automation cell assigned to a single VLAN to limit unnecessary traffic and allow network devices on the same VLAN to span multiple switches?
1524	Communication Protection	C800_82	Are VLANs configured to prohibit VLAN hopping?
1525	Communication Protection	C800_82	Are modems used in the callback mode?
1526	Communication Protection	C800_82	Are modems physically identified for control room operators to monitor?
1527	Communication Protection	C800_82	Are modems disconnected when not in use, and is there a timeout after a fixed period of inactivity?
1528	Communication Protection	C800_82	Do mesh networks use broadcast key versus public key management implemented at OSI Layer 2 (data link)?
1529	Communication Protection	C800_82	Is asymmetric cryptography used to perform administrative functions, and is symmetric encryption used to secure each data stream as well as network control traffic?
1530	Communication Protection	C800_82	Is an adaptive routing protocol used if the devices are used for wireless mobility?
1531	Communication Protection	C800_82	Is the convergence time of the network as fast as possible supporting rapid network recovery in the event of a failure or power loss?
1532	Communication Protection	C800_82	Are VPN devices thoroughly tested to verify that the technology is compatible with applications being used?

1533	Communication Protection	C800_82	Are VPN devices tested to ensure they do not unacceptably affect network traffic?
1534	Communication Protection	C800_82	Are firewalls deployed between the control system and corporate network?
1535	Firewall	C800_82	Do firewalls provide minimum connections to the corporate network such that the control system network can be severed from the corporate network in times of serious cyber incidents?
1537	Firewall	C800_82	Are sophisticated security implementations used between the control system and corporate networks?
1538	Firewall	C800_82	Is a firewall used in front of a router to implement logical network separation from the corporate network?
1539	Firewall	C800_82	Is there a DMZ with paired firewalls and are firewalls from different manufacturers used?
1540	Firewall	C800_82	Have communications delays been thoroughly analyzed and accounted for with the control system firewall implementation?
1541	Firewall	C800_82	Are firewall operations monitored to ensure that the firewall is performing its data collection tasks, and are the firewalls monitored on a real-time basis for rapid response to cyber incidents?
1542	Firewall	C800_82	Have all issues of firewall implementation been thoroughly considered such as the lack of experience in design of rule sets and the configuration of management issues associated with rule-set updates and deletions?
1543	Firewall	C800_82	Do the firewall rules provide source and destination filtering in addition to TCP and UDP port filtering and ICMP type and code filtering?
1544	Firewall	C800_82	Are all "permit" rules both IP address and TCP/UDP port specific and stateful (e.g., deep packet filtering and inspection), if appropriate?
1545	Firewall	C800_82	Do all rules restrict traffic to a specific IP address or range of addresses?
1546	Firewall	C800_82	Is any protocol allowed between the control network and DMZ explicitly prohibited between the DMZ and corporate networks (and vice versa)?
1547	Firewall	C800_82	Is all outbound traffic from the control network to the corporate network source and destination restricted by service and port?
1548	Firewall	C800_82	Are outbound packets from the control network or DMZ allowed only if those packets have a correct source IP address that is assigned to the control network or DMZ devices?
1549	Firewall	C800_82	Are control network devices prohibited to access the Internet?

1550	Firewall	C800_82	Is all firewall management traffic carried on either a separate, secured management network or over an encrypted network with multifactor authentication?
1551	Firewall	C800_82	Is firewall management traffic restricted by IP address to specific management stations?
1552	Firewall	C800_82	Are firewalls implemented to enforce security policy based on secure authentication of all users or processes seeking to gain access to the ICS network?
1553	Firewall	C800_82	Do firewalls enforce destination authorization based on user?
1554	Firewall	C800_82	Do firewalls record information flow for traffic monitoring, analysis, and intrusion detection?
1555	Firewall	C800_82	Are firewalls used to implement operational policies such as prohibition of email and permitted use of easy-to-remember usernames and group passwords?
1556	Firewall	C800_82	Is a stateful firewall implemented between the control system network and the corporate network and configured to deny all traffic except that which is explicitly authorized?
1557	Firewall	C800_82	Do firewalls inspect packets at the application layer and filter traffic based on specific application rules?
1558	Firewall	C800_82	Are firewalls implemented to block all communications with the exception of specifically enabled communications between devices on the unprotected LAN and protected control system networks?
1559	Access Control	C800_82	Are other cryptographic solutions such as cryptographic hashes considered in place of storing encrypted user passwords and authentication tokens?
1560	Communication Protection	C800_82	Is encryption at OSI Layer 2 (data link) considered/implemented rather than at Layer 3 (network) to reduce latency?
1561	Communication Protection	C800_82	Are record size increases considered with the use of encryption before deployment?
1562	Communication Protection	C800_82	Are key management issues considered before deployment of encryption?
1563	Communication Protection	C800_82	Are passwords encrypted in transit?
1564	Audit and Accountability	C800_82	Are the security auditors aware of the risks and consequences involved in testing the control system?
1565	Remote Access Control	C800_82	Are users accessing the control network from remote networks required to authenticate using an appropriately strong mechanism such as token-based authentication?

1566	Remote Access Control	C800_82	Are users required to authenticate a second time at the control network firewall using a strong mechanism such as a token based multi-factor authentication scheme?
1567	Communication Protection	C800_82	Is the noncontrol network traffic kept to the absolute minimum on an ICS network?
1568	Training	C800_82	Is feedback from the security awareness training used in revising the security plan?
1569	Communication Protection	C800_82	Is encryption used for device to device communication?
1570	Policies & Procedures General	Cfats	Are there documented and distributed cybersecurity policies, procedures, or plans?
1571	Policies & Procedures General	Cfats	Are there documented and distributed change management policies, procedures, or plans?
1572	Account Management	Cfats	Is the sharing of accounts prohibited?
1573	Account Management	Cfats	Are IT management, systems administration, and IT security duties divided among three different individuals?
1574	Monitoring & Malware	Cfats	Are networks monitored in near real time for unauthorized access or the introduction of malicious code?
1575	Audit and Accountability	Cfats	Are logs reviewed on a daily basis?
1576	Audit and Accountability	Cfats	Are alerts responded to in a timely manner?
1577	Incident Response	Cfats	Is the cyber incident response capability 24 × 7 × 365?
1578	Safety Instrumented System (SIS)	Cfats	Is the safety instrumented systems (SIS) in the facility with control systems configured so that they have no unsecured remote access and cannot be compromised through direct connections to the systems managing the processes they monitor?
1579	Configuration Management	Cfats	Is there a cohesive set of network/system architecture diagrams and other documentation including nodes, interfaces, and information flows?
1580	Audit and Accountability	Cfats	Are audits conducted at periodic intervals to determine whether the security objectives, measures, processes, and procedures conform to the identified information security requirements?
1581	Audit and Accountability	Cfats	Are audits conducted at periodic intervals to determine whether the security objectives, measures, processes, and procedures are effectively implemented and maintained?

1582	Audit and Accountability	Cfats	Are audits conducted at periodic intervals to determine whether the security objectives, measures, processes, and procedures perform as expected?
1583	Audit and Accountability	Cfats	Are system audit records reviewed and analyzed on a periodic frequency, and are findings reported to officials?
1586	Account Management	Components	Are accounts locked after a defined number of failed login attempts?
1587	Management Practices	Components	Are administrative default accounts, Administrator or root, renamed?
1588	Securing the Component	Components	Are all sample applications, toolkits, SDKs and unused virtual directories removed?
1589	Management Practices	Components	Are all unused, accounts, groups, and sites removed, e.g., Guest, Guests?
1590	Securing Content	Components	Are code reviews performed by a change committee and/or peer group to ensure there are no security or performance issues?
1591	Logging	Components	Are events, such as failed login attempts and failed file system actions, logged?
1592	System Protection	Components	Are host-based Intrusion Detection Systems (IDSs) used to alert administrators of anomalies?
1593	Password	Components	Are password defaults changed?
1594	Securing the Component	Components	Are portable media, such as CD-ROM drives, DVDs, floppy drives, or USBs, disabled or limited for use only by system administrators?
1596	Logging	Components	Are system administrators automatically notified of potential security threats, e.g., failed login attempts, failed file system activity, and malformed URL requests?
1597	Management Practices	Components	Are test and development servers located on a different network segment than the production servers?
1598	Securing the Component	Components	Are the OS and server located in separate logical or physical partitions from each other?
1599	Management Practices	Components	Are user and administrator account permissions/access based on least privilege principles?
1600	Securing Content	Components	Do application errors return a generic message rather than a detailed error?
1601	Logging	Components	Do logs get archived securely on another host for offline analysis?
1602	Password	Components	Does corporate policy support and enforce strong administrator and user passwords?
1603	Management Practices	Components	Does frequent and regular manual and/or automated security testing occur?

1604	Password	Components	Does the company have and enforce a policy for altering user and administrator passwords on a regular interval?
1605	Policies & Procedures General	Components	Does the company have and enforce a policy for locking out inactive user sessions?
1606	Policies & Procedures General	Components	Does the company have and enforce a policy for periodically applying security patches?
1607	Firewall	Components	Does the firewall rule set include a whitelist of approved users access, e.g., IP address restrictions, all others are refused?
1608	Firewall	Components	Does the firewall support Denial of Service (DoS) protection?
1609	User Authentication	Components	Does the system utilize an authentication mechanism such as Active Directory, LDAP, or a Kerberos server?
1610	Securing Content	Components	Has third-party code and applications been reviewed and approved by an authorized manager or committee?
1611	Policies & Procedures General	Components	Have all folder/file shares been reviewed and removed if not needed for critical processing?
1612	Firewall	Components	Have default ports been reviewed and modified to restrict noncritical traffic?
1613	Firewall	Components	Have open ports been reviewed and closed if they do not support critical business communications?
1614	Securing Content	Components	Have web servers, not designed for confidential information, been audited to ensure that business sensitive or personal information is not stored on the system?
1615	Management Practices	Components	Is an access banner displayed on computers providing notice that unauthorized use of the equipment may result in disciplinary action?
1616	Policies & Procedures General	Components	Is anti-malware software installed, running, and updated based on corporate policy?
1617	Securing Content	Components	Is delivery of business sensitive or personal information restricted to https only?
1618	Physical Access	Components	Are critical servers (domain controllers, application servers, PBX, video management systems) physically secure from unauthorized access? (i.e. located in a locked room)
1619	Remote Access Control	Components	Is remote access restricted to secure means only, such as AD secured, SSH, or 802.1X, and insecure methods such as VNC or telnet prohibited?
1620	Remote Access Control	Components	Is remote access user, access list, and where possible remote client restricted?
1621	Securing Content	Components	Is sensitive content isolated from other content?
1622	Password	Components	Passwords are not allowed to be reused?
1623	Securing the System	Components	Does the device sync system time to an accurate and reliable clock?

1624	Securing Content	Components	Are ad hoc queries disabled on production systems?
1625	Management Practices	Components	Are all sample database, toolkits, and SDKs removed?
1626	Securing the Component	Components	Are all services and processes not required by the application turned off, for example, FTP, POP3, SMTP, and VNC?
1627	Account Management	Components	Are all unused, accounts, groups and databases removed, e.g., Guest, Guests?
1628	Access Control	Components	Are application developers only given rights needed to develop applications and not full administrative permissions?
1629	Management Practices	Components	Are audits performed on a regular basis as defined by corporate policy for potential security and permission violations?
1630	Securing Content	Components	Are database backups stored securely, e.g., password protected and/or encrypted?
1631	Securing Content	Components	Are database communications secured, e.g., via SSL?
1632	Access Control	Components	Are individual users denied Data Definition Language (DDL) permissions?
1633	Securing the Component	Components	Are nonessential and unused administrative stored procedures, such an email or command shell, disabled?
1634	Boundary Protection	Components	Are public facing servers placed in a DMZ? In other words, behind a firewall with an additional firewall between that and any systems on the internal network?
1635	Access Control	Components	Are stored procedure permissions granted to roles only, e.g., not users?
1636	Management Practices	Components	Are the OS, database, and logs located in separate logical or physical partitions from each other?
1637	Securing Content	Components	Are unused link servers disabled?
1638	Securing the Component	Components	Are passwords or other sensitive server information removed from scheduled jobs, scripts, or queries? (particularly those in plain text format)
1639	Firewall	Components	Have database ports been set to nonstandard values, e.g., not 1433, 1521, or 3306?
1640	Securing Content	Components	Have default accounts such as Guest or Public been denied object permissions?
1641	User Authentication	Components	Is authentication via secure means, SSL or SSH only?
1642	Management Practices	Components	Is the database hosted on a dedicated server? In other words, are file, print, or Web servers capabilities hosted on separate physical or virtual servers?
1643	Encryption	Components	Are components or services that use clear text turned off or uninstalled?
1644	Communication Protection	Components	Are private VLANs, known as protected ports, used to secure sensitive communication over public or unsecure circuits?
1645	Management Practices	Components	Are users required to take security training before accessing the system?

1646	System Protection	Components	Do you employ an Intrusion Prevention System (IPS)?
1647	Policies & Procedures General	Components	Does the company have and enforce a policy for backing up critical software and data?
1648	Securing the Component	Components	Is a robust Uninterruptible Power Supply (UPS) utilized to minimize the impact of a power loss?
1649	Securing Content	Components	Is access to internal Web sites restricted to https?
1650	Encryption	Components	Are data communications to and from the node encrypted?
1651	Management Practices	Components	Does system access require two factor authentication?
1652	Management Practices	Components	Are all personal firewalls, those that are hosted on workstations and laptops, centrally administered?
1653	Boundary Protection	Components	Are loose and strict source routing blocked and logged?
1654	Policies & Procedures General	Components	Does the company have and enforce a policy for backing up firewall configurations?
1655	Policies & Procedures General	Components	Does the company have and enforce a policy for locking out inactive administrator sessions?
1656	Boundary Protection	Components	Has the egress firewall rules for the outbound traffic from the control network been reviewed and implemented?
1657	Boundary Protection	Components	Have rule sets been reviewed for appropriate order?
1658	Boundary Protection	Components	Have state tables been reviewed?
1659	Boundary Protection	Components	Is all incoming and outgoing ICMP traffic denied except where specifically permitted by your organization?
1660	Boundary Protection	Components	Is direct external traffic, traffic from the Internet, to critical servers blocked by default?
1661	Boundary Protection	Components	Is traffic to your e-mail server only allowed via a specific protocol and port?
1662	Management Practices	Components	Are annual audits performed to ensure that wireless devices have not been lost or stolen?
1663	Encryption	Components	Are device backups encrypted?
1664	Securing the Component	Components	Are devices labeled with the company name, address, and phone number in case the device is lost?
1665	Portable/Mobile/Wireless	Components	Are handheld devices stored in a secure location when not in use?
1666	Portable/Mobile/Wireless	Components	Are IR and Bluetooth capabilities disabled?

1667	Portable/Mobile/Wireless	Components	Are personal firewalls installed on handheld devices?
1668	Physical Access	Components	Are there physical access controls within buildings?
1669	Management Practices	Components	Are users prohibited from storing sensitive information on handheld devices?
1670	Portable/Mobile/Wireless	Components	Do handheld devices have a power on PIN code or password?
1671	Policies & Procedures General	Components	Does the company have and enforce a policy for disposing of devices, which include clearing permanent storage, such as hard drives, so that the data cannot be recovered?
1672	Management Practices	Components	Does the company have and enforce a policy for performing periodic inventory checks?
1673	Management Practices	Components	Does the organization keep a list of authorized device users?
1674	Management Practices	Components	Does training include how to safely store devices when not in use?
1675	Management Practices	Components	Does training include proper password selection?
1676	Management Practices	Components	Does training include the approved uses for company devices?
1677	Management Practices	Components	Does training include the type of information that the devices may store?
1678	Management Practices	Components	Does training include the type of programs that can be installed?
1679	Securing the Component	Components	Have the default “out-of-the-box” security settings been reviewed and modified?
1680	Portable/Mobile/Wireless	Components	Is antivirus software installed on a handheld wireless device?
1681	Portable/Mobile/Wireless	Components	Is business sensitive information stored on a handheld device encrypted?
1682	Securing the Component	Components	Is desktop application-mirroring software password protected?
1683	Management Practices	Components	Is there a disciplinary process that is enforced if a user misuses a device, and are users made aware of this process during their security training?

1684	Management Practices	Components	Is there a process to report lost or stolen devices, and are users made aware of this process during their security training?
1685	Management Practices	Components	Is wireless security training required of users before being issued a company handheld wireless device?
1686	Securing the System	Components	Are events logged and alerts issued if attack signatures are detected?
1687	Securing the System	Components	Are events logged and alerts issued if common attack profiles are detected?
1688	Securing the System	Components	Are events logged and alerts issued if protocol anomalies are detected?
1689	Securing the System	Components	Are events logged and alerts issued if tcp and udp port scans are detected?
1690	Securing the System	Components	Does administration, log transfers, and system updates to and from the device occur using secure protocols, such as HTTPS, SSH, SFTP, SNMPv3, and are all unsecure, clear text, communications disabled?
1691	Logging	Components	Does logging include, but is not limited to, critical host file changes, unauthorized and authorized client connection activity, and ad-hoc network creation?
1692	Securing the System	Components	Does the IDS include anomaly-based detection capabilities?
1693	Securing the System	Components	Does the IDS include host-based intrusion detection (HIDS) capabilities?
1694	Securing the System	Components	Does the IDS include network intrusion detection (NIDS) capabilities?
1695	Securing the System	Components	Does the IDS include root kit detection and mitigation?
1696	Securing the System	Components	Does the IDS include Signature-Based detection capabilities?
1697	Securing the System	Components	Does the IDS include stack-based detection (SIDS) capabilities?
1698	Securing the System	Components	Does the IDS include the ability to stop or mitigate known attack types?
1699	Securing the System	Components	Does the IDS issue timely alerts if system anomalies occur?
1700	Securing the System	Components	Does the IDS monitor its health and performance and issue alerts if there are problems?
1701	Securing the System	Components	Does the wireless network include wireless intrusion detection system (WIDS) capabilities?
1702	Securing the System	Components	Does the IPS include Anomaly Based prevention capabilities?
1703	Securing the System	Components	Does the IPS include host-based intrusion prevention (HIPS) capabilities?
1704	Securing the System	Components	Does the IPS include network behavior analysis (NBA) capabilities?
1705	Securing the System	Components	Does the IPS include network intrusion prevention (NIPS) capabilities?
1706	Securing the System	Components	Does the IPS include root kit prevention and mitigation?
1707	Securing the System	Components	Does the IPS include Signature-Based prevention capabilities?
1708	Securing the System	Components	Does the IPS include the ability to stop or mitigate known attack types?
1709	Securing the System	Components	Does the IPS monitor its health and performance and issue alerts if there are problems?

1710	Securing the System	Components	Does the IPS provide timely alerts if system anomalies occur?
1711	Securing the System	Components	Does the wireless network include wireless intrusion prevention system (WIPS) capabilities?
1712	Management Practices	Components	Are all login accounts except “root" removed?
1713	Encryption	Components	Are cryptographic keys changed periodically?
1714	Encryption	Components	Are cryptographic keys distributed according to recognized standards?
1715	Encryption	Components	Are cryptographic keys generated in accordance with a specified algorithm and key size using recognized standards?
1716	Encryption	Components	Are cryptographic keys managed according to recognized standards?
1717	Securing the Component	Components	Are file transfers disabled?
1718	Management Practices	Components	Does the company have and enforce a remote access policy which is verified through assessments?
1720	Encryption	Components	Has the link encryption been confirmed to meet company or external security standards?
1721	Securing the Component	Components	Is only confirmed trustworthy software allowed to be executed?
1722	Remote Access Control	Components	Is remote command execution disabled?
1723	Remote Access Control	Components	Is remote login disabled?
1724	Logging	Components	Are all incoming connections logged?
1725	Management Practices	Components	Are modems configured based on a corporate policy?
1726	Remote Access Control	Components	Are modems, DSL, or other network backdoor access points for third party vendors or partners disabled when not needed?
1727	Remote Access Control	Components	Are remote dial access numbers periodically changed?
1728	Remote Access Control	Components	Do you use a different range of phone numbers for the office than the IDS modem pool?
1729	Management Practices	Components	Does the login screen display banner information according to corporate security policies?

1730	Remote Access Control	Components	Is a telecom firewall implemented?
1731	Remote Access Control	Components	Is auto answer disabled on modems when not needed?
1732	Logging	Components	Is the callback option enabled?
1733	Remote Access Control	Components	Modems are not attached to any type of server?
1734	Securing Content	Components	Are data removed from the printer disk or memory after a print operation?
1735	Encryption	Components	Are network printer communications encrypted?
1736	Securing the Component	Components	Are network printers, other than those required for continuous control system operations, locked after a period of user inactivity?
1737	Communication Protection	Components	Are network protocols that aren't being used turned off?
1738	Securing Content	Components	Are printer hard drives encrypted?
1739	Securing the Component	Components	Are sensitive communications to the Network Printer protected via a trusted communication path? NOTE: This also includes FAX ports on multifunction printers. The FAX ports should be restricted to only FAX-related activities.
1740	Securing Content	Components	Has a job timeout been set?
1741	Access Control	Components	Have access control lists been implemented?
1742	Securing the Component	Components	Have Internet print capabilities, e.g., IPP or FTP, been turned off?
1743	Securing the Component	Components	Have you implemented Denial of Service (DoS) protection?
1744	Securing Content	Components	IF the capability exists, has a PIN system been implemented for print authorization?
1745	Securing the Component	Components	If the printer has a hard drive, is remote access to the drive disabled?
1746	Physical Access	Components	Is access to internal printer hardware restricted?
1747	Securing the Component	Components	Is the Network Printer capable of automatic restart after a service discontinuity, and is the capability enabled?
1748	Securing Content	Components	On print error, is disk or memory dumped?
1749	Firewall	Components	Are ports 80 and 443, http and https respectively, closed?
1750	Encryption	Components	Are optical ring communications encrypted?
1751	Management	Components	Are access rules added, modified, and deleted as business needs change?

1752	Logging	Components	Are authentication and administrative events, including enabling and disabling logging, recorded?
1753	Policies & Procedures General	Components	Are firmware patches reviewed and applied in a timely fashion as defined by the corporate security policy?
1754	Securing the Router	Components	Are IP directed broadcasts disallowed?
1755	Securing the Router	Components	Are local user accounts disabled on the router?
1756	Securing the Router	Components	Are TCP & UDP small services disallowed?
1757	Securing the Router	Components	Are the device's incoming packets sourced with invalid addresses disallowed?
1758	Securing the Router	Components	Do routers use an authentication service (i.e. TACACS+, Kerberos, LDAP) for all user authentications?
1759	Securing the Component	Components	If SNMP is not used, are SNMP community strings erased and the service disabled?
1760	Securing the Component	Components	Is IP source routing disallowed?
1761	Securing the Router	Components	Is remote access to routers restricted to SSH, e.g., no telnet?
1762	Password	Components	Is the enabled password on the device kept in a secure encrypted format?
1763	Safety Instrumented System (SIS)	Components	Does the Safety Instrument System (SIS) have its own inputs and actuators, separate from the industrial control system (ICS)?
1764	Safety Instrumented System (SIS)	Components	Has a hazard operations study to determine SIL (Safety Integrity Level) been performed?
1765	Safety Instrumented System (SIS)	Components	Has a review been conducted to ensure that all components are designed to the determined SIL (Safety Integrity Level)?
1766	Safety Instrumented System (SIS)	Components	Is the SIS isolated from the process control network?
1767	Remote Access Control	Components	Are terminal servers NOT installed on any type of domain controller?
1768	Remote Access Control	Components	Has an approved application, e.g., white list, been established and implemented?
1769	Management	Components	Is a single terminal server devoted to each shared application?
1770	Encryption	Components	Is communication between clients and the terminal server encrypted?
1771	Remote Access Control	Components	Is the terminal server remote control feature disabled?
1772	Securing the Component	Components	Is the unidirectional device employed certified to a rigorous and reliable standard, for example, to CC EAL +7?

1773	Communication Protection	Components	Are local user accounts disabled on the VLAN router?
1774	Securing the Component	Components	Are MAC addresses security features implemented?
1775	Communication Protection	Components	Has a VLAN ID been dedicated for all trunk ports?
1776	Securing the Component	Components	Has Auto-trunking been disabled?
1777	Communication Protection	Components	Has Cisco Discovery Protocol (CDP) been disabled?
1778	Securing the Component	Components	Has Spanning Tree Attack (STP) mitigation been implemented?
1779	Communication Protection	Components	Have Address Resolution Protocol (ARP) security issues been mitigated?
1780	Communication Protection	Components	Have all disabled ports been put in an unused VLAN?
1781	Securing the Component	Components	Have all unused ports been disabled?
1782	Securing the Component	Components	Have dynamic trunk (virtual trunk) features been disabled?
1783	Communication Protection	Components	Have switch ports been isolated so that no traffic from other ports can be delivered to an isolated or private VLAN port?
1784	Communication Protection	Components	Is VLAN 1 NOT used for anything?
1785	Communication Protection	Components	Is VLAN Trunk Protocol (VTP) used?
1786	Access Control	Components	Are common user accounts given limited privileges on company-owned computers?
1787	Securing the Component	Components	Are email clients configured to prevent automatic loading of remote email images, limit mobile code execution, default message is plain text, automatic previewing is disabled, and spam filtering enabled?
1788	Securing the Component	Components	Are Instant Messaging (IM) clients configured so that display of email addresses is suppressed and file transfers are restricted?
1789	Securing the Component	Components	Are office productivity suites configured so that macro use is restricted, personal information is limited, and secured folders are used to store document files?

1790	Securing Content	Components	Are only company-owned PCs used for telework or remote access?
1791	Policies & Procedures General	Components	Are personal computer firewalls enabled and configured according to company policy?
1792	Policies & Procedures General	Components	Are remote access users required to re-authenticate their credentials as stipulated by the corporate security policy.
1793	Remote Access Control	Components	Are remote sessions disconnected after 30 minutes of inactivity?
1794	Securing the Component	Components	Are unneeded networking features disabled?
1795	Password	Components	Are user accounts protected with passwords?
1796	Physical Access	Components	Are user sessions protected from unauthorized physical access?
1797	Policies & Procedures General	Components	Are web browsers used for telework configured to restrict cookies, block popups, enable anti-phishing, remove unneeded browser plug-ins, set a master password to protect stored information, and run programs with the least privileges possible?
1798	Policies & Procedures General	Components	Before disposing of a telework client device or remote access server, does the organization remove any sensitive data from it?
1799	Management Practices	Components	Does the organization regularly perform operational processes to maintain telework and remote access security, including deploying updates, verifying clock synchronization, reconfiguring access control as needed, and detecting and documenting anomalies within the remote access infrastructure?
1800	Policies & Procedures General	Components	Is a different brand of Web browser used for telework?
1801	Securing Content	Components	Is disk storage encrypted on the telework devices?
1802	Policies & Procedures General	Components	Is remote access software configured according to the company's security policies?
1803	Policies & Procedures General	Components	Is the use of remote access utilities stipulated and enforced based on the corporate security policy?
1804	Portable/Mobile/Wireless	Components	Is wireless networking configured to automatically connect to available networks?
1805	Management	Components	Is workstation content filtering software installed and enabled?
1806	Securing Content	Components	Are any folders given execute and write permissions?
1807	Securing Content	Components	Are CGI execute permissions restricted to only those folders that require them?
1808	Access Control	Components	Are read/write permissions denied to files and folders that do not require these permissions?

1809	Management	Components	Are the Operating System (OS) and applications, data and database, and logs loaded on separate logical or physical partitions?
1810	Securing the Component	Components	If there is no file extension, does the system return a 404 error?
1811	Policies & Procedures General	Components	Is read/write ability restricted to only those services and processes that require this access?
1812	Remote Access Control	Components	Is remote user access restricted, e.g., no remote root login, restricted remote access list, and where possible restricted remote client?
1813	User Authentication	Components	Is Web-based authentication via SSL or TLS only?
1814	Securing Content	Components	Are “dual connected” devices, such as computers that have both wireless and hardwire connectivity, prohibited?
1815	Communication Protection	Components	Are Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES) used with a minimum key length of 128 bits to secure wireless routers?
1816	Management Practices	Components	Are there standardized security configurations for client devices and access points?
1817	Management Practices	Components	Does the company have and enforce a policy for performing security assessments of the organization’s wireless network on a regular basis?
1818	Securing Content	Components	For those “dual connected” devices that are approved, have software-based controls that permit either wireless or wired network access, but not both simultaneously, been installed?
1819	Securing Content	Components	For those devices that are not approved for wireless access, has the BIOS been configured so that wireless connections are automatically terminated when a wired connection is detected?
1820	Portable/Mobile/Wireless	Components	Has the default SSID wireless router name been changed?
1821	Portable/Mobile/Wireless	Components	Has the Service Set Identifier (SSID) broadcast been disabled on the wireless router?
1822	Communication Protection	Components	Is either the Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) used as the authentication protocol?
1823	Securing Content	Components	Is interference between wireless access deployments avoided?
1824	Management Practices	Components	Is the wireless network installed, supported, and maintained by an approved support team?

1825	Securing Content	Components	Is there a separate wireless network for visitors to use?
1826	Securing Content	Components	Is wireless access based on a list of hardware addresses (MAC address) that can be registered and tracked?
1827	Management Practices	Components	Is wireless security configuration implementation and maintenance standardized, automated, and centralized?
3443	Account Management	Components	Are Active Directory domains used to restrict or allow user or group permissions?
3444	Account Management	Components	Do you use Active Directory to enforce authentication policies? (e.g. password complexity, lockout on failed attempts, password expiration)
3445	Remote Access Control	Components	Have you audited and eliminated backdoor remote access connections?
3446	Account Management	Components	Have Active Directory DNS administrators groups been set up to manage DNS?
3447	Account Management	Components	Are the DNS administrators groups and users placed into a designated Organizational Unit (OU) with appropriate Group Policy applied?
3448	Boundary Protection	Components	Is the DNS server co-located with the AD server? (i.e., not across a WAN or slow-speed link).
3449	Account Management	Components	Are Active Directory permissions configured to be compatible ONLY with the version of Windows used?
3451	Password	Components	Are robust passwords (e.g., length, complexity) used to access administrator accounts?
3452	Account Management	Components	Have domain administrators (members of the Domain Admins group and the built-in Administrator account) been limited to a small, controlled group?
3455	Management Practices	Components	Is the Active Directory SYSKEY stored externally (i.e. USB, CD, etc.) rather than on the local hard drive?
3456	Management Practices	Components	Is there a backup domain controller available if the primary domain controller fails?
3457	Boundary Protection	Components	Have separate Active Directory domains been created to separate security or administrative functions (e.g. separate domains for corporate and ICS networks)?
3458	Account Management	Components	Have all default user and computer objects been moved into OUs with the correct permissions?
3459	Management Practices	Components	Have you implemented an Active Directory policy to log changes to security configurations and failed attempts to access system resources?

3460	System and Communications Protection	Components	Has the network traffic for group policy object (GPO) refresh, password changes, and time synchronization been evaluated for network loading?
3461	Recover	Components	Is there a current active directory object map to perform an authoritative restore in case an object is maliciously deleted?
3462	Password	Components	Has the Directory Services Restore Mode (DSRM) password been set utilizing robust passwords (e.g., length, complexity)?
3463	System Integrity	Components	Are you using a DNS server?
3467	Boundary Protection	Components	Are system components (IP cameras, PBX, domain controllers, servers, modems, switches, routers, etc.) protected from external networks by a firewall?
3468	Password	Components	Have default user names and passwords for system components (IP cameras, PBX, domain controllers, servers, modems, switches, routers, etc.) been changed utilizing robust passwords (e.g., length, complexity)?
3469	System and Communications Protection	Components	Is security camera traffic properly secured when routed over an unsecured network (e.g. Internet)?
3470	Audit and Accountability	Components	Is video storage protected from power interruptions?
3471	Audit and Accountability	Components	Are IP cameras included in the system component audit?
3473	Access Control	Components	Do you have any access agreements (formal or informal) for third party access to your telephone (PBX) system?
3475	Configuration Management	Components	Is port security used on the VoIP Network particularly publicly accessible jacks?
3476	Communication Protection	Components	Are IP phones and PBX secured behind a VoIP ready firewall?
3478	System and Communications Protection	Components	Are voicemail messages and unified communications physically secure from unauthorized access? (ex: located in a locked room with limited access.)
3480	Audit and Accountability	Components	Are VoIP handsets included in system audits?
3481	System and Communications Protection	Components	Is voice and data traffic separated?

3482	Remote Access Control	Components	Are VPN tunnels used to secure remote access connections outside of the facility?
3483	Encryption	Components	Does your VoIP system encrypt phone calls?
3484	System Integrity	Components	Do you deploy patches for your VoIP equipment, including firmware updates on the handsets themselves?
3485	Physical Access	Components	Are critical network components (modems, switches, routers, firewalls) physically secure from unauthorized access? (i.e. located in a locked room)
3486	Password	Components	Have default user names and passwords for administration been changed utilizing robust password guidelines (e.g., length, complexity)?
3487	Encryption	Components	Has WPA2 been implemented as the encryption type?
3488	Configuration Management	Components	Has the default SSID been changed?
3489	Configuration Management	Components	Has MAC address filtering been enabled?
3490	Configuration Management	Components	Has SSID broadcasting been disabled according to company policy?
3491	System Integrity	Components	Do you have procedures in place for patch deployment, including firmware updates?
3841	System and Services Acquisition	DODI_8510	Does the organization require the developer of the information system, system component, or information system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization exactly as specified by the master copies?
3842	System and Services Acquisition	DODI_8510	Does the organization use independence criteria to verify if an independent assessor has implemented a correct assessment plan and collected related assessment evidence?
3843	System and Services Acquisition	DODI_8510	Does the organization require the developers of the system, system components, or system services to test software against organizationally-defined criteria?
3844	System and Services Acquisition	DODI_8510	Does the organization require the developer of the system to perform attack surface reviews?
3845	System and Services Acquisition	DODI_8510	Does the organization require the system developer to verify that the security testing scope provides complete coverage and depth?
3846	System and Services Acquisition	DODI_8510	Does the organization conduct an assessment of the system prior to selection, acceptance, or update?
3847	System and Services Acquisition	DODI_8510	Does the organization use all-source intelligence analysis of suppliers of the system, system component, or system service?

3848	System and Services Acquisition	DODI_8510	Does the organization use Operations Security (OPSEC) safeguards to protect supply chain-related information for the system, components, or services?
3849	System and Services Acquisition	DODI_8510	Does the organization implement security safeguards to validate that the system or component is genuine?
3850	System and Services Acquisition	DODI_8510	Does the organization establish agreements and procedures with supply chain organizations that provide systems, components, or services?
3851	System and Services Acquisition	DODI_8510	Does the organization employ security safeguards to ensure an adequate supply of system components?
3852	System and Services Acquisition	DODI_8510	Does the organization establish identification of supply chain elements, processes, and actors for system, components, or services?
3853	System and Services Acquisition	DODI_8510	Does the organization create a process to fix deficiencies in supply chain elements that have been identified during an assessment?
3854	System and Services Acquisition	DODI_8510	Does the organization require the developer of the information system, component, or service to define quality metrics at the beginning of the development process?
3855	System and Services Acquisition	DODI_8510	Does the organization require the developer of the system, component, or service to validate quality metrics on a defined frequency or upon delivery?
3856	System and Services Acquisition	DODI_8510	Does the organization require the developer of the system to select and deploy a security tracking tool for use during development?
3857	System and Services Acquisition	DODI_8510	Does the organization require the developer of the system to perform criticality analysis in the system development life cycle?
3858	System and Services Acquisition	DODI_8510	Do developers perform threat modeling and vulnerability analysis for the system using organizational parameters, tools, methods, and evidence?
3859	System and Services Acquisition	DODI_8510	Does the organization require the developer of the system to reduce attack surfaces to company defined thresholds?
3860	System and Services Acquisition	DODI_8510	Does the organization require the developer of the system to implement an explicit process to continuously improve the development process?
3861	System and Services Acquisition	DODI_8510	Does the organization require the developer of the system to perform automated vulnerability analysis, determine exploitation potential, determine potential risk mitigation, and deliver results to company defined roles?
3862	System and Services Acquisition	DODI_8510	Does the organization require the developer of the system to use threat modeling and vulnerability analyses on similar systems as guidance for the current development process?
3863	System and Services Acquisition	DODI_8510	Does the organization require the developer of the system to provide an incident response plan?

3864	System and Services Acquisition	DODI_8510	Does the organization require the developer of the system to produce a formal security policy model that is consistent and sufficient when elements are implemented?
3865	System and Services Acquisition	DODI_8510	Does the organization require the developer of the system to define security-relevant elements and provide a rational that it is complete?
3866	System and Services Acquisition	DODI_8510	Does the organization require the developer of the system to produce formal specifications for security-relevant interfaces to the system and provide proof that it is consistent with the formal policy model?
3867	System and Services Acquisition	DODI_8510	Does the organization require the developer of the system to demonstrate that the formal top-level specification completely covers the security-relevant interfaces and that it is an accurate description?
3868	System and Services Acquisition	DODI_8510	Does the organization require the developer of the system to describe the security-relevant elements not addressed in the formal top-level specification? (i.e. internal security-relevant elements)
3869	System and Services Acquisition	DODI_8510	Does the organization require the developer of the system to produce informal specifications for security-relevant interfaces to the system and that it is consistent with the formal policy model?
3870	System and Services Acquisition	DODI_8510	Does the organization require the developer of the system to demonstrate that the descriptive top-level specification completely covers the security-relevant interfaces and that it is an accurate description?
3871	System and Services Acquisition	DODI_8510	Does the organization require the developer of the system to describe the security-relevant elements not addressed in the formal top-level specification?
3872	System and Services Acquisition	DODI_8510	Does the organization require the developer of the system to structure security-relevant hardware, software, and firmware to integrate simple protection mechanisms with fine configuration granularity?
3873	System and Services Acquisition	DODI_8510	Does the organization require the developers of the system to structure security-relevant elements to facilitate testing?
3874	System and Services Acquisition	DODI_8510	Does the organization implement a tamper protection program for the system?
3875	System and Services Acquisition	DODI_8510	Does the organization employ anti-tamper technologies and techniques throughout the system development life cycle?
3876	System and Services Acquisition	DODI_8510	Does the organization inspect systems, components, or devices, regularly or at random in order to detect tampering?

3877	System and Services Acquisition	DODI_8510	Does the organization have an anti-counterfeit policy and procedure and is it effective at preventing counterfeit components from entering the system?
3878	System and Services Acquisition	DODI_8510	Is justification provided for continued use of an unsupported component in the system?
3879	System and Communications Protection	DODI_8510	Does the system audit the identity of internal users associated with denied communications?
3880	System and Communications Protection	DODI_8510	Does the organization prevent unauthorized physical connections across the boundary protections?
3881	System and Communications Protection	DODI_8510	Does the system route all remote accesses through a managed interface for access control and auditing?
3882	System and Communications Protection	DODI_8510	If the boundary protection device fails does the system fail in a secure mode?
3883	System and Communications Protection	DODI_8510	Does the system block both inbound and outbound traffic between all clients independently configured by end users and external service providers?
3884	System and Communications Protection	DODI_8510	Does the system isolate or segregate organization defined system components from other components of the system as needed?
3885	System and Communications Protection	DODI_8510	Does the organization use boundary protection mechanisms to separate system components?
3886	System and Communications Protection	DODI_8510	Does the system obscure feedback of protocol format validation failures?
3887	System and Communications Protection	DODI_8510	Does the system employ techniques to randomize or conceal communication unless otherwise protected by physical mechanisms?
3888	System and Communications Protection	DODI_8510	Does the system provide a trusted communication path that is identifiable from other paths?

3889	System and Communications Protection	DODI_8510	Are systems configured to prohibit remote activation of collaborative computing (e.g., IM, video conferencing) and is there an indication of use to the local user?
3890	System and Communications Protection	DODI_8510	Does the system identify who is present in all VTC and IP based online meetings?
3891	System and Communications Protection	DODI_8510	Does the system prevent the download and execution of unacceptable mobile code as defined by mobile code requirements?
3892	System and Communications Protection	DODI_8510	Does the system allow the use of certificate authorities for verification of the session?
3893	System and Communications Protection	DODI_8510	Does the system protect the confidentiality and integrity of all nonpublic information?
3894	System and Communications Protection	DODI_8510	Does the system implement cryptography to prevent disclosure and modification of all information outside of organization facilities?
3895	System and Communications Protection	DODI_8510	Are concealment and misdirection techniques used to confuse and mislead adversaries used in protecting the system at an organization defined time period?
3896	System and Communications Protection	DODI_8510	Are organizational techniques used to introduce randomness into organizational operations and assets?
3897	System and Communications Protection	DODI_8510	Does the organization change location of processing and storage at organization defined time intervals?
3898	System and Communications Protection	DODI_8510	Does the organization reduce bandwidth for identified covert channels or storage to organizationally-defined values?
3899	System and Communications Protection	DODI_8510	Does the organization protect the integrity of information prior to and after storage on read-only media?

3900	System and Communications Protection	DODI_8510	Does the organization employ hardware based protection of system firmware components?
3901	System and Communications Protection	DODI_8510	Does the organization ensure that only organization individuals or system can receive the information, system components, or devices?
3902	System and Communications Protection	DODI_8510	Does the system use cryptographic mechanisms to protect from intentional electromagnetic interference?
3903	System and Communications Protection	DODI_8510	Does the system use cryptographic mechanisms to reduce the detection potential of wireless links?
3904	System and Information Integrity	DODI_8510	Does the organization install security-relevant software and firmware updates within 30 days or according to organizational policy?
3905	System and Information Integrity	DODI_8510	Does the system detect, audit, and prevent execution of unauthorized commands at a console?
3906	System and Information Integrity	DODI_8510	Does the system employ security measures to authenticate remote commands?
3907	System and Information Integrity	DODI_8510	Does the organization use tools and techniques to analyze malicious code and uses the results to enhance incident response and flaw remediation processes?
3908	System and Information Integrity	DODI_8510	Does the organization analyze outbound communications at the boundary and interior of the system to detect covert exfiltration?
3909	System and Information Integrity	DODI_8510	Does the organization implement additional monitoring of new users?
3910	System and Information Integrity	DODI_8510	Does the system monitor for unauthorized network services and alerts organization defined personnel when found?

3911	System and Information Integrity	DODI_8510	Are host-based monitoring mechanisms at system components implemented?
3912	System and Information Integrity	DODI_8510	Does the system perform integrity checks of software, firmware, and data at startup or at intermediate states or security events on an organizationally-defined frequency?
3913	System and Information Integrity	DODI_8510	Upon detection of an integrity violation, does the system perform actions to document the event and notify organizational personnel?
3914	System and Information Integrity	DODI_8510	Is the integrity of boot firmware in defined devices protected?
3915	System and Information Integrity	DODI_8510	Is spam protection automatically updated by the system?
3916	System and Information Integrity	DODI_8510	Does the system check all external facing application software inputs that might receive an exploit? (e.g., web/application servers, database servers, etc)
3917	System and Information Integrity	DODI_8510	Is there a manual override on the system that is restricted to authorized users, allows for input validation and creates audit records when used?
3918	System and Information Integrity	DODI_8510	Is mean time to failure of system components used in a failure prevention strategy?
3919	System and Information Integrity	DODI_8510	Are software and data used by system components and services reloaded from organizational defined sources?
3920	System and Information Integrity	DODI_8510	Does the system validate information output from software to ensure that it is consistent with the expected content?
2874	Risk Management and Assessment	INGAA	Do you implement physical security according to the INGAA AGA document specifically as it relates to 49 CFR Parts 192 and 193, and according to the pre-TSA document “Security Practices Guidelines Natural Gas Industry Transmission and Distribution,” revised May 2008?

2875	System Protection	INGAA	Have you established personnel security requirements including security roles and responsibilities for third-party providers?
2876	Physical Security	INGAA	Have you established a secure method of monitoring?
2877	Portable/Mobile/Wireless	INGAA	Do you audit the use, access, and necessity of these connections, and base its monitoring and periodic review on company policy?
2878	Risk Management and Assessment	INGAA	Is the network infrastructure secured to prevent the unauthorized installation of wireless technology?
2879	Risk Management and Assessment	INGAA	Is the wireless connectivity included in network documentation, policies, and procedures?
2880	Risk Management and Assessment	INGAA	Do you, at a minimum, conduct an annual review, reassessment, and update of the control systems cybersecurity plans in accordance with the operator's policy?
2881	Risk Management and Assessment	INGAA	Where the responsible entity cannot conform to its own cybersecurity policy, do you document these instances as exceptions, and are they authorized according to company policy?
2882	Risk Management and Assessment	INGAA	Are the criticality classification of cyber assets as defined in Section 3.2 reviewed at least every 18 months?
2883	Organizational	INGAA	Is the methodology used to define critical assets, the classification of critical assets, and the classification of critical cyber assets reviewed, approved, and documented according to company policy?
2884	System and Services Acquisition	INGAA	Have you defined a cross-functional cybersecurity team and an operational framework to ensure coordination, communication, and accountability for information security on and between the control systems and enterprise networks?
2885	System and Services Acquisition	INGAA	Have you defined information and cybersecurity roles, responsibilities, and lines of communication among the operations, IT, and business groups, as well as with outsourcers, partners, and third-party contractors?
2886	Configuration Management	INGAA	Have you established a system and services acquisition policy, procurement standards, and a process by which potential acquisitions are evaluated against the standards, including encouraging the vendor to follow software development standards for trustworthy software throughout the development life cycle?
2887	Configuration Management	INGAA	Does the company develop and document a network security coordination process?
2888	Policies	INGAA	Does the network security coordination process include a delineation of roles and responsibilities associated with coordination, communication, and accountability of information security on and between the control systems and enterprise networks?

2889	Plans	INGAA	Does the network security coordination process define information security coordination requirements at every step of the systems development life cycle including strategic planning, design, acquisition, testing, installation, configuration/change management, and retirement?
2890	Plans	INGAA	Does the cybersecurity team establish and document a framework in accordance with company policy that defines the security organization and the roles, responsibilities, and accountabilities of the system owners and users?
2891	Plans	INGAA	Does your company ensure the implementation of bi-directional lines of communication no matter what structure is in place between the systems owners and users?
2892	Plans	INGAA	Are the lines of communication between system owners and users documented and exercised to test and ensure their effectiveness?
2893	Access Control	INGAA	Has the company established a control system and services acquisition policy, procurement standards, and a process by which potential systems, components, and service acquisitions are evaluated against the standards, in accordance with company policy?
2894	Access Control	INGAA	Does your company encourage the vendor to follow software development standards for trustworthy software throughout the development life cycle.
2895	System Integrity	INGAA	Does your procurement standards include system hardening?
2896	System Integrity	INGAA	Does your procurement standards include perimeter protections?
2897	System Integrity	INGAA	Does your procurement standards include account management?
2898	System Integrity	INGAA	Does your procurement standards include coding practices?
2899	System Integrity	INGAA	Does your procurement standards include flaw remediation?
2900	System Integrity	INGAA	Does your procurement standards include malware detection and protection?
2901	Configuration Management	INGAA	Does your procurement standards require that providers of control system services employ security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements?
2902	Continuity	INGAA	Does your procurement standards define oversight and user roles and responsibilities with regard to external information system services?
2903	Monitoring & Malware	INGAA	Does your procurement standards define oversight and user roles and responsibilities with regard to monitors security control compliance by external service providers?

2904	Monitoring & Malware	INGAA	Does the life cycle section of your cybersecurity plan address the incorporation of security measures and controls into the cyber system design and operation for both new system creation and legacy system modification?
2905	Configuration Management	INGAA	Does the life cycle section of your cybersecurity plan address mitigation strategies for security deficiencies found in control system components?
2906	System Protection	INGAA	Does the life cycle section of your cybersecurity plan address the implementation of policies and procedures for the assessment and maintenance of system status and configuration information including tracking changes made to the control systems network, and patching and upgrading operating systems and applications?
2907	Physical Security	INGAA	Does the life cycle section of your cybersecurity plan address the implementation of policies and procedures for the secure disposal of equipment and associated media?
2908	System Integrity	INGAA	Have you developed and documented the practices and procedures that would incorporate cybersecurity into the control systems design, modification, and operation?
2909	System Integrity	INGAA	Is cybersecurity consideration part of the initial specification and design of new control systems and all changes to existing systems?
2910	Physical Security	INGAA	Do all new control system operation practices and procedures incorporate cybersecurity consideration?
2911	Monitoring & Malware	INGAA	Do all existing practices and procedures include appropriate cybersecurity considerations?
3168	Risk Management and Assessment	INGAA	Has the organization completed a determination of cyber assets that are classified as Critical Cyber Assets?
3169	Policies	INGAA	The control system security policy should prohibit the embedding of sensitive passwords in source code, scripts, aliases, and short-cuts. If necessary, encryption techniques should be used.
3170	Policies	INGAA	Do you secure your source code to prevent both its unauthorized viewing and modification?
3171	Policies	INGAA	Are your control systems' hosts and workstations only used for approved control system activities?
3172	Policies	INGAA	Do you run any new protocol, application, or software proposed to be added to the control system network in a test-bed or development environment to evaluate the potential for impairing the performance of the control system?

3173	Policies	INGAA	Do you only grant the minimum set of rights, privileges, or accesses required by users or processes to perform any control system operation, maintenance, or monitoring task?
3174	Policies	INGAA	Do you enable audit logging for all devices that are capable?
3175	Policies	INGAA	Do you periodically review all rights, privileges, and accesses for all users or process to all control system components and resources including but not limited to physical access, OS services, files, disks, shared data, and networking resources to ensure that unauthorized changes have not been made?
3176	Policies & Procedures General	INGAA	Do you review all control systems operational procedures to ensure cybersecurity policies are maintained at design levels?
3177	Policies & Procedures General	INGAA	Do you have policies and procedures for addressing hardware and software security deficiencies in control systems?
3178	Procedures	INGAA	Do you have procedures for hardening all components used in control systems.
3179	Procedures	INGAA	Do you have procedures for securing the configurations for all network devices such as firewalls, routers, and switches and used to establish baseline configuration for these devices?
3180	Procedures	INGAA	Do you review the baseline system configurations including services and ports periodically based on company policy to ensure that unauthorized changes have not been made?
3181	Procedures	INGAA	Do you remove or disable the operating system services that are not used by the production SCADA to reduce the risk of being exploited?
3182	Procedures	INGAA	Do you review the enabled networking protocols on all networked devices and disable unessential protocols should be disabled?
3183	Procedures	INGAA	Do you document all required applications and open ports both for normal operation and emergency operation?
3184	Procedures	INGAA	Do you disable all port and applications not in use?
3185	Procedures	INGAA	Do you perform a risk assessment on system services to see if the benefits of having them running outweigh the potential for exploitation?
3186	Procedures	INGAA	Do you only allow remote functions that an operating system provides when necessary and only use secure versions?
3187	Procedures	INGAA	Do you discourage the use of FTP on a SCADA system and strictly control it?
3188	Procedures	INGAA	Do you disable or otherwise protect removable media devices (USB ports, CD/DVD drives, and other removable media devices)?
3189	Procedures	INGAA	Do you remove the guest accounts?

3190	Procedures	INGAA	Do you change the default passwords?
3191	Procedures	INGAA	Do you disallow unhardened devices on the network?
3192	Procedures	INGAA	Do you use secure coding techniques when developing applications?
3193	Procedures	INGAA	Do you strictly control administrative access to all control systems?
3194	Procedures	INGAA	Do you require strong passwords for administrative accounts?
3195	Procedures	INGAA	Do you change passwords periodically based on company policy and whenever personnel changes dictate?
3196	Procedures	INGAA	Do you have policies and procedures for management of software patches and updates, antivirus software, and anti-malware software?
3197	Procedures	INGAA	Do you apply all critical control system supplier approved operating system updates in accordance with company policy?
3198	Procedures	INGAA	Do you use antivirus, anti-malware, and other protection software in accordance with the control system supplier's recommendations?
3199	Procedures	INGAA	Do you periodically inventory the software patch level of all systems on the network to be aware of unpatched systems based on company policy?
3200	Procedures	INGAA	Do you ensure that critical application and database security patches are applied in accordance with the control system supplier recommendations?
3201	Procedures	INGAA	Do your change control policies and procedure address any change that will impact the pipeline control system whether permanent or temporary?
3202	Procedures	INGAA	Do you use some type of document control?
3203	Procedures	INGAA	Do you use a baseline change approach that fully documents the control system configuration?
3204	Procedures	INGAA	Do you have procedures to recover the baseline configuration in the event of unexpected impacts or failures from the changes made to the baseline configuration?
3205	Procedures	INGAA	Do you follow the process steps as outlined in Section 3.3.3.3?
3206	Procedures	INGAA	Have you established policies and procedures for the secure disposal of equipment and associated media and does it include the sanitization of information system media, both digital and nondigital, prior to disposal or release for reuse?
3207	Plans	INGAA	Does your control system cybersecurity plans address plans and preparation for the return to full service of unavailable, degraded, or compromised control systems in a timely fashion as defined by the organization consistent with their availability and recovery requirements?
3208	Plans	INGAA	Do you plan and prepare for the prompt restoration and recovery of a failed or compromised SCADA system?

3209	Plans	INGAA	Do you have plans that include contingencies for cyber threats, natural disasters, and/or equipment/software failures?
3210	Procedures	INGAA	Do you have procedures for restoring systems from backups?
3211	Procedures	INGAA	Does your employee training ensure familiarization with the contents of the plans?
3212	Procedures	INGAA	Do your procedures define the roles and responsibilities of first responders?
3213	Procedures	INGAA	Do you have communication procedures and a list of personnel to contact in the case of an emergency, including control system vendors, network administrators, and control system support personnel?
3214	Procedures	INGAA	Do you have procedures for validating system backups?
3215	Plans	INGAA	Does the restoration and recovery plan include references to current configuration information on all systems requiring restoration?
3216	Plans	INGAA	Does the restoration and recovery plan include specifications of recovery time objectives and specific contingency plan objectives if recovery times are exceeded?
3217	Plans	INGAA	Does the restoration and recovery plan include a required response to events or conditions of varying duration and severity that would activate the recovery plan?
3218	Plans	INGAA	Does the restoration and recovery plan include a personnel list for authorized physical and cyber access to the control system?
3219	Plans	INGAA	Does the restoration and recovery plan include requirements for the timely replacement of components in the case of an emergency?
3220	Plans	INGAA	Do you review the plan periodically according to company policy?
3221	Plans	INGAA	Do you make and secure backups of critical system software, including applications, data, and configuration information, on a regular basis as defined by company policy consistent with their availability and recovery requirements?
3222	Plans	INGAA	Do you keep Installation media and license information in a secure location?
3223	Plans	INGAA	Do you test the restoration and recovery process periodically according to company policy, which includes executing it on a frequency according to company policy and reviewing and refining as necessary according to company policy?
3224	Plans	INGAA	Does your CSP control system cybersecurity plan include the implementation of policies and procedures for cyber intrusion monitoring, detection, incident handling, and reporting?
3225	Plans	INGAA	Do you establish policies and procedures for cyber intrusion monitoring and detection as well as incident handling and reporting?
3226	Policies	INGAA	Do your monitoring procedures include unexpected log file events?
3227	Policies	INGAA	Do your monitoring procedures include unusually heavy network traffic?

3228	Policies	INGAA	Do your monitoring procedures include out of disk space or significantly reduced free disk space?
3229	Policies	INGAA	Do your monitoring procedures include unusually high CPU usage?
3230	Policies	INGAA	Do your monitoring procedures include creation of new user accounts?
3231	Policies	INGAA	Do your monitoring procedures include attempted or actual use of administrator-level accounts?
3232	Policies	INGAA	Do your monitoring procedures include locked-out accounts?
3233	Policies	INGAA	Do your monitoring procedures include account in-use when the user is not at work?
3234	Policies	INGAA	Do your monitoring procedures include cleared log files?
3235	Policies	INGAA	Do your monitoring procedures include full log files with unusually large number of events?
3236	Policies	INGAA	Do your monitoring procedures include antivirus alerts?
3237	Policies	INGAA	Do your monitoring procedures include disabled antivirus software and other security controls?
3238	Policies	INGAA	Do your monitoring procedures include unexpected patch changes?
3239	Policies	INGAA	Do your monitoring procedures include machines connecting to outside IP addresses?
3240	Policies	INGAA	Do your monitoring procedures include requests for information about the system (social engineering attempts)?
3241	Policies	INGAA	Do your monitoring procedures include unexpected changes in configuration settings?
3242	Policies	INGAA	Do your monitoring procedures include unexpected system shutdown?
3243	Policies	INGAA	Does your organization have cyber incident handling and procedures?
3244	Policies	INGAA	Does your incident response plan include Roles and Responsibilities Definition?
3245	Policies	INGAA	Does your incident response plan include Declaration of Preparation?
3246	Policies	INGAA	Does your incident response plan include Incident Response Phases Definition?
3247	System Protection	INGAA	Does the organization develop and enforce policies and procedures where control system workstations are only used for approved activities?
3249	Physical Security	INGAA	Are non-critical facilities access controls implemented to the same protection standards as the main facility?
3250	Access Control	INGAA	Does the enhanced access control in the security plan include consideration of physical and logical access, risk assessment of wireless implementation, and access to Critical Cyber Assets?

3251	Physical Security	INGAA	Does the organization implement physical access controls as specified in regulatory sources? (i.e., INGAA Pipeline Security Practices Guidelines Natural Gas Pipeline Industry Transmission and Distribution)
3347	Configuration Management	NCSF_V1	Is there a defined list of software programs authorized to execute on the system?
3348	Risk Management and Assessment	NCSF_V1	Does the organization map all communication and data flows?
3349	Remote Access Control	NCSF_V1	Are all external information systems catalogued?
3350	Plans	NCSF_V1	Are the organization's place in critical infrastructure and its industry sector identified and communicated?
3351	Plans	NCSF_V1	Does the organization have a plan for critical infrastructure recovery developed and tested?
3352	Policies	NCSF_V1	Does your organization have an Information and Document Management Policy?
3353	Policies	NCSF_V1	Does your organization have a Media Protection Policy?
3354	Policies	NCSF_V1	Does your organization have a System Security Policy?
3355	Access Control	NCSF_V1	Does your organization have an Access Control Policy?
3356	Policies	NCSF_V1	Does your organization have an Audit and Accountability Policy?
3357	Policies	NCSF_V1	Does your organization have a Cryptographic Policy?
3358	Policies	NCSF_V1	Does your organization have an Identification and Authentication Policy?
3359	Policies	NCSF_V1	Does your organization have a Monitoring and Review Policy?
3360	Policies	NCSF_V1	Does your organization have a System and Communication Protection Policy?
3361	Policies	NCSF_V1	Does your organization have a System and Services Acquisition Policy?
3362	Training	NCSF_V1	Do privileged users understand their roles and responsibilities in cybersecurity?
3363	Training	NCSF_V1	Do senior executives understand their roles and responsibilities with regard to security?
3364	Training	NCSF_V1	Do physical security personnel, through training and testing, understand their roles and responsibilities in regard to cybersecurity?
3365	Configuration Management	NCSF_V1	Does your organization have a Configuration Management Plan?
3366	Communication Protection	NCSF_V1	Does the organization share with industry partners proven effective protection technologies?
3367	Continuity	NCSF_V1	Does the continuity of operations plan include necessary notifications to stakeholders?

3368	Continuity	NCSF_V1	Does the organization understand the impact of the cyber incident?
3369	Incident Response	NCSF_V1	Do personnel have knowledge of cyber forensics and execute them in accordance with the incident response plan?
3370	Incident Response	NCSF_V1	Are cybersecurity incidents categorized according to the incident response plan?
3371	Incident Response	NCSF_V1	Are cybersecurity incidents contained according to the incident response plan?
3372	Incident Response	NCSF_V1	Are cybersecurity incidents mitigated according to the incident response plan?
3373	Risk Management and Assessment	NCSF_V1	Are new vulnerabilities mitigated or documented as acceptable risks?
3374	Continuity	NCSF_V1	Are lessons learned incorporated into recovery plans?
3375	Continuity	NCSF_V1	Is the recovery plan reviewed and updated to address lessons learned, system, organizational, and technology changes?
3376	Continuity	NCSF_V1	Does the organization attempt to restore company reputation after an event is repaired?
3378	Risk Management and Assessment	NCSF_V1	Are risk management procedures developed, managed and distributed to the organizational members?
3379	Risk Management and Assessment	NCSF_V1	Does the organization use risk information from similar industries to determine its own risk tolerance?
3380	Risk Management and Assessment	NCSF_V1	Are information and systems categorized in accordance with business risk, policies, regulations, standards, and guidance?
3381	Risk Management and Assessment	NCSF_V1	Are the security categorization results documented and prioritized in the system security plan?
3382	System and Services Acquisition	NCSF_V1	Is organization's place in critical infrastructure and its industry sector is identified and communicated?
3383	Incident Response	NCSF_V1	Have the organization's upstream and downstream dependencies been identified in the supply chain?
3384	Info Protection	NCSF_V1	Are organizational mission, objectives and activities determined and prioritized according to organization time period?
3385	Environmental Security	NCSF_V1	Does the organization have critical services such as communications, internet provider, or electrical power that are needed for critical functioning of the business?
3386	Environmental Security	NCSF_V1	Does the organization use UPS or generators as sources of alternate power to support critical business processes?
3387	Continuity	NCSF_V1	Does the organization use an alternate telecommunications provider to provide critical business services?
3388	Continuity	NCSF_V1	Does the organization test whether alternate critical functions are adequate?

3389	Communication Protection	NCSF_V1	Does the organization have adequate supply of materials to continue to provide delivery of critical business service?
3390	Continuity	NCSF_V1	Does the organization understand resilience as it applies toward re-establishing critical services?
3391	Plans	NCSF_V1	Has capacity planning determined the necessary capacity for information processing, telecommunications, and environmental support needed during restoration operations?
3392	Continuity	NCSF_V1	Is there a formal, documented resilience planning policy for the system that addresses critical services?
3393	Plans	NCSF_V1	Are risk-reduction mitigation measures identified and prioritized?
3394	Risk Management and Assessment	NCSF_V1	Is there a detailed mitigation strategy for individual systems that addresses risk and is there a comprehensive strategy?
3395	Policies	NCSF_V1	Does the organization manage user names and credentials for each user or device contained in the system?
3396	Procedures	NCSF_V1	Do you have procedures for issuing a name and password for each user in all systems?
3397	Account Management	NCSF_V1	Are system accounts authorized, established, activated, modified, disabled, and removed according to the organization defined time period?
3398	Account Management	NCSF_V1	Is there a minimum password complexity of defined requirements for case sensitivity, number of characters, mix of upper case letters, lower case letters, numbers, and special characters, including minimum requirements for each type and are passwords required to be changed in an organization-defined time period?
3399	Audit and Accountability	NCSF_V1	Is there sufficient storage capacity allocated to reduce the likelihood of such capacity being exceeded?
3400	Plans	NCSF_V1	Has capacity planning determined the necessary capacity for information processing, telecommunications, and environmental support needed for daily operations?
3401	Procedures	NCSF_V1	Do you have a configuration change control plan?
3402	Remote Access Control	NCSF_V1	Is cryptography used to protect the confidentiality and integrity of remote access sessions? (See FIPS 140 for validated cryptographic modules)
3403	Monitoring & Malware	NCSF_V1	Are automated tools used to support near real-time analysis of events and are these events analyzed for after-the-fact examples of attack targets and methods?
3404	Incident Response	NCSF_V1	Are system network security incidents tracked and used to correlate with other sensors and system log files?
3405	Monitoring & Malware	NCSF_V1	Are vulnerability scans performed on a defined frequency or randomly in accordance with organizational policy?

3406	Monitoring & Malware	NCSF_V1	If vulnerability scanning tools are unavailable, is the organization able to compensate using passive monitoring tools?
3407	Risk Management and Assessment	NCSF_V1	Are the results of periodic, unannounced, in-depth monitoring or penetration testing used to improve detection processes?
3408	Risk Management and Assessment	NCSF_V1	Are the results of system monitoring used as a basis for improving detection processes?
3409	Monitoring & Malware	NCSF_V1	Are vulnerability scanning tools updated and improved?
2912	Account Management	NEI_0809	Are CDA accounts managed and documented to include: authorizing, establishing, activating, modifying, reviewing, disabling and removing accounts?
2913	Account Management	NEI_0809	Are CDA accounts managed and reviewed against the access control list at least every 31 days?
2914	Account Management	NEI_0809	Are computer automated mechanisms used to manage CDA accounts in activities such as terminate, disable inactive accounts within 31 days, create and protect audit records, and notify system administrator of account modifications?
2915	Access Control	NEI_0809	Does the organization conduct reviews of job function changes to ensure account rights remain limited to job function?
2916	Access Control	NEI_0809	Does the organization define and document privileged functions and security relevant information on the CDA?
2917	Access Control	NEI_0809	Does the organization document and enforce access mechanisms (e.g. passwords) that do not adversely impact the operational performance of CDAs and employs alternate compensating security controls when access enforcement cannot be used?
2918	Access Control	NEI_0809	When access enforcement mechanisms may adversely impact the performance of CDAs, do you document and employ alternate security controls when access enforcement is unavailable?
2919	Access Control	NEI_0809	Does the organization restrict access to privileged functions and security information to authorized personnel?
2920	Communication Protection	NEI_0809	Does the organization document information flow control enforcement by using protected processing level (e.g., defensive architecture) as a basis for flow control decisions?
2921	Access Control	NEI_0809	Does the organization enforce separation of CDA functions through assigned access authorizations?

2922	Access Control	NEI_0809	Does the organization implement alternative controls and document the justification where a CDA cannot support differentiation of roles and where a single individual must perform all roles within the CDA?
2923	Access Control	NEI_0809	Does the organization implement alternative controls and document the justification for alternative controls/countermeasures for increased auditing where a CDA cannot support the differentiation of privileges within the CDA and where an individual must perform all roles within the CDA?
2924	Access Control	NEI_0809	Does the organization document the justification and details for alternative controls/countermeasures where a CDA cannot support account/node locking or delayed login attempts?
2925	Access Control	NEI_0809	Does the organization ensure that CDA "Use Notification" provides privacy and security notices?
2926	Access Control	NEI_0809	Does the organization implement alternative controls and document the justification for alternative controls/countermeasures where a CDA cannot support session locks? And ensures that the CDA is protected from unauthorized access, monitored, audited, and has verification of qualified personnel access?
2927	Info Protection	NEI_0809	Does the organization identify and implement standard naming conventions for identification of special dissemination, handling, or distribution instructions in compliance with 10 CRF 2.390 and 10 CFR 73.21?
2928	Portable/Mobile/Wireless	NEI_0809	Does the organization disable wireless capabilities when not utilized?
2929	System Integrity	NEI_0809	Does the organization perform verification during deployment of CDAs, when changes or modifications occur to CDAs, and every 31 days for accessible areas and that CDAs are free of insecure connections such as vendor connections and modems?
2930	Portable/Mobile/Wireless	NEI_0809	Does the organization enforce and document that mobile device security and integrity are maintained at a level consistent with the CDA they support?
2931	Access Control	NEI_0809	Is information that could cause an adverse impact on SSEP functions or could assist an adversary in carrying out an attack not released to the public?
2932	Audit and Accountability	NEI_0809	Where a CDA cannot support the use of automated mechanisms to generate audit records, are there alternative controls and documented justification for alternative controls or countermeasures?
2933	Audit and Accountability	NEI_0809	Does the organization coordinate security audit functions within the facility to enhance mutual support and help guide the selection of auditable events?

2934	Audit and Accountability	NEI_0809	Does the CDA prevent users from altering or destroying audit records?
2935	Audit and Accountability	NEI_0809	Does the organization meet NRC record retention requirements?
2936	Audit and Accountability	NEI_0809	Does the CDA or security boundary device failover to a redundant CDA, where necessary, to prevent adverse impact to safety, security or emergency preparedness functions?
2937	Audit and Accountability	NEI_0809	Does the CDA or security boundary device, when necessary, respond during failure by overwriting the oldest audit record or records?
2938	Audit and Accountability	NEI_0809	Is the failure of audit processing capabilities attributed as a failure of the CDA or security boundary device?
2939	Audit and Accountability	NEI_0809	Does the organization review and analyze CDAs audit records every 31 days, for indications of in appropriate or unusual activity, and report the findings to the designated official?
2940	Audit and Accountability	NEI_0809	Does the organization document the justification and details for alternate compensating security controls where a CDA cannot support auditing reduction and report generation by providing this capability through a separate system?
2941	Audit and Accountability	NEI_0809	Does the organization ensure CDAs use a time source protected at an equal or greater level than the CDAs or internal system clocks to generate time stamps for audit records, and the time on CDAs are synchronized?
2942	Communication Protection	NEI_0809	Does the organization document procedures that facilitate the implementation of the CDA, system, and communications protection policy?
2943	Communication Protection	NEI_0809	Does the organization implement alternative controls and document the justification for alternative controls/countermeasures for individuals who have access to the CDA are qualified, trustworthy, and reliable per 10 CFR 73.56?
2944	Communication Protection	NEI_0809	Does the organization implement alternative controls and document the justification for alternative controls/countermeasures for physically restricted access to the CDA and timely detection and response to intrusions?
2945	Communication Protection	NEI_0809	Does the organization implement alternative controls and document the justification for alternative controls/countermeasures where a CDA cannot internally support transmission confidentiality capabilities through ensuring that individuals who have access to the CDA are qualified, trustworthy, and reliable per 10 CFR 73.56?

2946	Communication Protection	NEI_0809	Does the organization implement alternative controls and document the justification for alternative controls/countermeasures where a CDA cannot internally support transmission confidentiality capabilities through physical restrictions, monitoring, and record physical access to the CDA?
2947	Communication Protection	NEI_0809	Does the organization manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures when cryptography is required and employed within the CDAs in accordance with NEI 0809 Rev 6 Appendix D Section 3.9 (NRC Regulatory Issue Summary (RIS) 2002-15, Revision 1)?
2948	Communication Protection	NEI_0809	Are CDAs configured to provide physical disconnection of cameras and microphones in a manner that supports ease of use except where these technologies are used to control and monitor the CDA for security purposes?
2949	Communication Protection	NEI_0809	Does the organization configure CDAs so they, upon receipt of data, perform data origin authentication and data integrity verification on resolution responses whether or not CDAs request this service?
2950	Physical Security	NEI_0809	Is physical access to CDAs restricted?
2951	Access Control	NEI_0809	Does the organization implement the strongest possible challenge-response authentication mechanism where domain-based authentication is not used?
2952	Account Management	NEI_0809	Are passwords changed every 92 days and have length and complexity for the required security?
2953	Account Management	NEI_0809	On a CDA that cannot support device identification and authentication, are alternative controls implemented and documented with justification for using alternative controls?
2954	Access Control	NEI_0809	Does the organization ensure that CDAs authenticate cryptographic modules in accordance with NEI 08-09 Rev 6 Appendix D Section 3.9 (NRC Regulatory Issue Summary (RIS) 2002-15, Revision 1)?
2955	System Integrity	NEI_0809	Does the organization verify and document that CDAs are patched or mitigated in accordance with the patch management process and security prioritization timelines?
2956	System Integrity	NEI_0809	Does the organization document the level of support for testing patch releases?
2957	Info Protection	NEI_0809	Does the media protection policy and procedures detail the purpose, scope, roles, responsibilities, management commitment, coordination among entities, and compliance for information categories as defined by the site policies?
2958	Info Protection	NEI_0809	Does the media protection procedures include the methodology that defines the purpose, scope, roles, responsibilities, and management commitment in the areas of media receipt, storage, handling, sanitization, removal, reuse, and disposal?

2959	Info Protection	NEI_0809	Is CDA testing with storage media verified every 92 days to ensure equipment and procedures are functioning properly?
2960	Personnel	NEI_0809	Does a certifying official grant access prior to an individual gaining access to CDAs or communication systems?
2961	Personnel	NEI_0809	Does the organization retrieve information (e.g. security-related and organizational) formerly controlled by terminated or transferred individual?
2962	Personnel	NEI_0809	Are qualified individuals proven to be trustworthy and reliable in accordance with 10 CFR 73.56?
2963	System Integrity	NEI_0809	Where a CDA cannot support the use of automated mechanisms for the management of distributed security testing, is there justification and documentation for employing alternative or compensating controls?
2964	System Integrity	NEI_0809	Does the organization perform scans to verify the integrity, operation and functions of software and information every 92 days?
2965	Physical Security	NEI_0809	Does the organization develop, implement and document a plan for CDAs located outside of the protected area in regard to physical security protection, roles, responsibilities and management accountability, organization's staff, third-party contractors, and environmental protection?
2966	Physical Security	NEI_0809	Does the organization include personnel security controls in acquisition-related contract and agreement documents?
2967	Physical Security	NEI_0809	Does the organization implement physical security controls to limit access to CDAs and to prevent degradation of the operational environment?
2968	Physical Security	NEI_0809	Does the organization control and document visitor access to CDAs by verifying the identity and confirming access authorization prior to entry?
2969	Physical Security	NEI_0809	Does the organization employ secure management communications and encryption per Appendix D of NEI 08-09, Rev 6?
2970	Physical Security	NEI_0809	Does the organization ensure that direct communications between digital assets at lower security levels and digital assets at higher security levels are eliminated or restricted (e.g. relating to defense-in-depth) with justification that explains that communication from a lower security level to a higher security level verifies that a compromise of such communication will not prevent or degrade the functions performed by the CDAs in the higher security level?

2971	Incident Response	NEI_0809	Are the incident response team members identified and do they represent the following organizations: Physical security, Cyber security team, Operations, Engineering, Information Technology, Human resources, System support vendors, Management, Legal, and Safety?
2972	Continuity	NEI_0809	Are backups of CDAs tested at an interval of no less than 31 days?
2973	Organizational	NEI_0809	Does the situational awareness training include understanding normal behavior of the CDA so that abnormal behavior is recognized?
2974	Configuration Management	NEI_0809	Does the organization establish configuration management security controls for CDAs with the process described in Section 4.2 of Cyber Security Plan?
2975	Configuration Management	NEI_0809	Are the up-to-date baseline configurations audited every 92 days?
2976	Configuration Management	NEI_0809	Does the organization document the justification for alternate (compensating) security controls where a CDA cannot support the use of automated mechanisms to centrally manage, apply, and verify configuration settings?
2977	System and Services Acquisition	NEI_0809	Does the organization develop a formal, documented procedure to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls?
2993	Access Control	NEI_0809	Does the system authenticate devices before establishing connections to CDAs?
2994	Monitoring & Malware	NEI_0809	Is unauthorized use of CDAs identified? (e.g., log monitoring)
2995	Audit and Accountability	NEI_0809	Are changes to CDAs consistent with your configuration management program?
1180	Risk Management and Assessment	Nerc_Cip_R3	control centers and backup control centers?
1181	Risk Management and Assessment	Nerc_Cip_R3	transmission substations that support the reliable operation of the Bulk Electric System?
1182	Risk Management and Assessment	Nerc_Cip_R3	consider generation resources that support the reliable operation of the Bulk Electric System?
1183	Risk Management and Assessment	Nerc_Cip_R3	systems and facilities critical to system restoration?
1184	Risk Management and Assessment	Nerc_Cip_R3	systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more?
1185	Risk Management and Assessment	Nerc_Cip_R3	Special Protection Systems that support the reliable operation of the Bulk Electric System?

1186	Risk Management and Assessment	Nerc_Cip_R3	any additional assets that support the reliable operation of the Bulk Electric System?
1187	System Protection	Nerc_Cip_R3	Have the critical cyber assets been identified, reviewed, and updated on at least an annual basis?
1188	Policies & Procedures General	Nerc_Cip_R3	Has the control systems specific cybersecurity policy been disseminated to those with a need to know?
1189	Organizational	Nerc_Cip_R3	Is the change in senior management leadership documented within 30 calendar days of the effective date?
1190	Organizational	Nerc_Cip_R3	Does the senior manager delegate authority for specific actions to a named delegate or delegates, and are the delegations documented by name, title, and date of designation and approved by the senior manager?
1191	Organizational	Nerc_Cip_R3	Has the senior manager or delegate(s) authorized and documented any exception from the requirements of the cybersecurity policy?
1192	Policies & Procedures General	Nerc_Cip_R3	Have conformance issues with the cybersecurity policy been documented as exceptions and authorized by the senior manager or delegate(s)?
1193	Policies & Procedures General	Nerc_Cip_R3	Are exceptions to the cybersecurity policy documented within 30 days of senior manager or delegate(s) approval?
1194	Policies & Procedures General	Nerc_Cip_R3	Are exceptions to the cybersecurity policy documented with an explanation as to necessity and any compensating measures?
1195	Policies & Procedures General	Nerc_Cip_R3	Are exceptions to the cybersecurity policy reviewed and approved annually by the senior manager or delegate(s) to ensure they are still valid and required?
1196	Risk Management and Assessment	Nerc_Cip_R3	Does the critical cyber asset information to be protected include operational procedures, lists as required in Standard CIP-002-3, network topology, floor plans that contain critical cyber assets, equipment layouts of critical cyber assets, disaster recovery plans, incident response plans, and security configuration information?
1197	Info Protection	Nerc_Cip_R3	Are personnel who authorize access to protected information identified by name, title, and information for which they are responsible for authorizing access?
1198	Info Protection	Nerc_Cip_R3	Is the list of personnel responsible for authorizing access to protected information verified at least annually?
1200	Info Protection	Nerc_Cip_R3	Are the processes for controlling access privileges to protected information assessed at least annually?
1201	Training	Nerc_Cip_R3	Does training material include policies, access controls, and procedures for critical cyber assets?

1202	Training	Nerc_Cip_R3	Does training include the proper use of critical cyber assets, physical and electronic access controls to critical cyber assets, the proper handling of critical cyber asset information, and action plans and procedures to recover or re-establish critical cyber assets and access following a cyber security incident?
1203	Personnel	Nerc_Cip_R3	Does the personnel assessment include an identity verification and 7-year criminal check?
1204	Personnel	Nerc_Cip_R3	Are the results of personnel risk assessments documented, and are personnel risk assessments of contractor and service vendor personnel conducted pursuant to Standard CIP-004-3?
1205	Personnel	Nerc_Cip_R3	Is the list of personnel who have access to critical cyber assets reviewed quarterly, and is the list updated within 7 calendar days of any change of personnel or any change in the access rights?
1206	Communication Protection	Nerc_Cip_R3	Is there a defined electronic security perimeter for dial-up accessible critical cyber assets that use nonroutable protocols?
1207	Communication Protection	Nerc_Cip_R3	Are end points of communication links connecting discrete electronic security perimeters considered access points and included in the electronic security perimeter?
1208	Communication Protection	Nerc_Cip_R3	Are noncritical cyber assets within a defined electronic security perimeter identified and protected pursuant to the requirements of Standard CIP-005-3?
1209	Communication Protection	Nerc_Cip_R3	Are access control and monitoring assets of the electronic security perimeter afforded protective measures as specified in CIP-003-3, CIP-004-3 Requirement R3, CIP-005-3 Requirements R2 and R3, CIP-006-3 Requirements R2 and R3, CIP-007-3 Requirements R1 and R3 through R9, CIP-008-3, and CIP-009-3?
1210	Communication Protection	Nerc_Cip_R3	Is there documentation of electronic security perimeter(s), all interconnected critical and noncritical cyber assets within the electronic security perimeter(s), all electronic access points to the electronic security perimeter(s), and the cyber assets deployed for the access control and monitoring of these access points?
1211	Communication Protection	Nerc_Cip_R3	Is there a procedure for securing dial-up access to the electronic security perimeter(s)?
1212	Monitoring & Malware	Nerc_Cip_R3	Is there a documented monitoring process(es) at each dial-up access point device?
1213	Monitoring & Malware	Nerc_Cip_R3	Does the vulnerability assessment include a document identifying the vulnerability assessment process?

1214	Monitoring & Malware	Nerc_Cip_R3	Does the vulnerability assessment include a process of discovery for access points in the electronic security perimeter?
1215	Configuration Management	Nerc_Cip_R3	Is the documentation updated to reflect the modification of the network or controls within 90 calendar days of the change?
1216	Access Control	Nerc_Cip_R3	Are electronic access logs retained for at least 90 calendar days, and are logs related to reportable incidents kept in accordance with the requirements of Standard CIP-008-3?
1217	Plans	Nerc_Cip_R3	Is there a documented, implemented, and maintained physical security plan approved by the senior manager or delegate(s)?
1218	Physical Security	Nerc_Cip_R3	Do all cyber assets within an electronic security perimeter also reside in a physical security perimeter OR are alternative measures deployed and documented to control physical access to such cyber assets?
1219	Plans	Nerc_Cip_R3	Does the physical security plan address update of the physical security plan within 30 calendar days of the completion of any physical security system redesign or reconfiguration?
1220	Plans	Nerc_Cip_R3	Does the physical security plan address annual review of the physical security plan?
1221	Physical Security	Nerc_Cip_R3	Do cyber assets that authorize and/or log access to the physical security perimeter(s) have the protective measures specified in Standard CIP-003-3; Standard CIP-004-3, Requirement R3; Standard CIP-005-3, Requirements R2 and R3; Standard CIP-006-3, Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3?
1222	Physical Security	Nerc_Cip_R3	Do cyber assets used in the access control and/or monitoring of the electronic security perimeter(s) reside within an identified physical security perimeter?
1223	Physical Security	Nerc_Cip_R3	Does logging record sufficient information to uniquely identify individuals and the time of access 24 hours a day, 7 days a week?
1224	Physical Security	Nerc_Cip_R3	Are there documented technical and procedural mechanisms for logging physical entry at all access points to the physical security perimeter(s)?
1225	Physical Security	Nerc_Cip_R3	Are electronic physical access logs produced OR Is electronic capture of video images used for logging physical access, and are they of sufficient quality to determine identity OR Is manual logging of physical access used and maintained by security as specified in Requirement R4?
1226	Physical Security	Nerc_Cip_R3	Are physical access logs retained for at least 90 calendar days, and are logs related to reportable incidents kept in accordance with the requirements of Standard CIP-008-3?

1227	Physical Security	Nerc_Cip_R3	Is there a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly?
1228	Physical Security	Nerc_Cip_R3	Are all physical security systems tested and maintained on a cycle no longer than 3 years?
1229	Physical Security	Nerc_Cip_R3	Are all physical security systems testing and maintenance records retained for the cycle identified in accordance with Requirement R8.1.
1230	Physical Security	Nerc_Cip_R3	Are all physical security systems outage records regarding access controls, logging, and monitoring retained for a minimum of 1 calendar year?
1231	System Protection	Nerc_Cip_R3	Is there a documented process to ensure that only those ports and services required for normal and emergency operations are enabled?
1232	System Integrity	Nerc_Cip_R3	Is the assessment of security patches and security upgrades for applicability documented within 30 calendar days of availability of the patches or upgrades?
1233	System Integrity	Nerc_Cip_R3	Is the implementation of security patches documented?
1234	System Integrity	Nerc_Cip_R3	Are compensating measures applied to mitigate risk exposure documented when patches are not installed?
1235	Monitoring & Malware	Nerc_Cip_R3	Are antivirus and malware prevention tools documented and implemented?
1236	Account Management	Nerc_Cip_R3	Are user accounts implemented as approved by designated personnel per CIP-003-3 Requirement R5?
1237	Account Management	Nerc_Cip_R3	Are there methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of 90 days?
1238	Account Management	Nerc_Cip_R3	Are user accounts reviewed at least annually to verify access privileges are in accordance with CIP-003-3 R5 and CIP-004-3 R4 requirements?
1239	Account Management	Nerc_Cip_R3	Is there a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges, including factory default accounts?
1240	Account Management	Nerc_Cip_R3	Are individuals with access to shared accounts identified?
1241	Access Control	Nerc_Cip_R3	Are passwords changed at least annually?
1242	Info Protection	Nerc_Cip_R3	Are data storage media erased prior to redeployment?
1243	Risk Management and Assessment	Nerc_Cip_R3	Is there a document identifying the vulnerability assessment process?

1244	Risk Management and Assessment	Nerc_Cip_R3	Does the vulnerability assessment verify that only ports and services required for operation of the cyber assets within the electronic security perimeter are enable?
1245	Risk Management and Assessment	Nerc_Cip_R3	Does the vulnerability assessment review the controls for default accounts?
1246	Risk Management and Assessment	Nerc_Cip_R3	Is the documentation specified in Standard CIP-007-3 reviewed and updated at least annually, including ensuring changes resulting from modifications to the systems or controls are documented within 30 calendar days of the change?
1247	Incident Response	Nerc_Cip_R3	Does the incident response plan include a process for reporting incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC)?
1248	Incident Response	Nerc_Cip_R3	Are all reportable cybersecurity incidents reported to the ES-ISAC either directly or through an intermediary?
1249	Incident Response	Nerc_Cip_R3	Is documentation related to cybersecurity incidents reportable per Requirement R1.1 retained for 3 calendar years?
1250	Continuity	Nerc_Cip_R3	Are updates to the recovery plan(s) communicated to personnel responsible for the activation and implementation of the recovery plan(s) within 30 calendar days of the change being completed?
1251	Risk Management and Assessment	Nerc_Cip_R4	Does the critical cyber asset information to be protected include operational procedures, lists as required in Standard CIP-002-4, network topology, floor plans that contain critical cyber assets, equipment layouts of critical cyber assets, disaster recovery plans, incident response plans, and security configuration information?
1252	Personnel	Nerc_Cip_R4	Are the results of personnel risk assessments documented, and are personnel risk assessments of contractor and service vendor personnel conducted pursuant to Standard CIP-004-4?
1253	Communication Protection	Nerc_Cip_R4	Are noncritical cyber assets within a defined electronic security perimeter identified and protected pursuant to the requirements of Standard CIP-005-4a?
1254	Communication Protection	Nerc_Cip_R4	Are access control and monitoring assets of the electronic security perimeter afforded protective measures as specified in CIP-003-4, CIP-004-4 Requirement R3, CIP-005-4a Requirements R2 and R3, CIP-006-4c Requirements R2 and R3, CIP-007-4 Requirements R1 and R3 through R9, CIP-008-4, and CIP-009-4?
1255	Access Control	Nerc_Cip_R4	Are electronic access logs retained for at least 90 calendar days and are logs related to reportable incidents kept in accordance with the requirements of Standard CIP-008-4?

1256	Physical Security	Nerc_Cip_R4	Do cyber assets that authorize and/or log access to the physical security perimeter(s) have the protective measures specified in Standard CIP-003-4; Standard CIP-004-4, Requirement R3; Standard CIP-005-4a, Requirements R2 and R3; Standard CIP-006-4c, Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4?
1257	Physical Security	Nerc_Cip_R4	Are physical access logs retained for at least 90 calendar days, and are logs related to reportable incidents kept in accordance with the requirements of Standard CIP-008-4?
1258	Risk Management and Assessment	Nerc_Cip_R4	Is the documentation specified in Standard CIP-007-4 reviewed and updated at least annually, including ensuring changes resulting from modifications to the systems or controls are documented within 30 calendar days of the change?
3413	Configuration Management	Nerc_Cip_R5	Has the Responsible Entity identified and classified high, medium and low impact BES Cyber systems according to CIP-002-5 Attachment 1, Section 1?
3414	Configuration Management	Nerc_Cip_R5	Does the Responsible Entity review the identification Requirement R1 (CIP-002-5.1) and update changes at least every 15 calendar months even if no changes are required?
3415	Organizational	Nerc_Cip_R5	Is there a review process for high and medium impact BES Cyber Systems and is it updated at least once every 15 calendar months and does a CIP Senior manager approve it?
3416	Organizational	Nerc_Cip_R5	Is there a documented review process for high and medium impact BES Cyber Systems and does the process include topics addressed in CIP-003-5 Parts 1.1 through 1.9?
3417	Organizational	Nerc_Cip_R5	Are low impact BES Cyber Security Systems reviewed at least once every 15 calendar months in a manner that identifies, assesses, and corrects deficiencies?
3418	Organizational	Nerc_Cip_R5	Does the review of low impact BES Cyber Systems address cyber security topics from CIP-003-5 R2 Part 2.1 through Part 2.4 and is it approved by management?
3419	Organizational	Nerc_Cip_R5	Is the CIP Senior Manager identified by name and documented within 30 calendar days of any change?
3420	Organizational	Nerc_Cip_R5	Are changes to the delegation of authority document approved by the CIP Senior Manager and updated within 30 days?
3421	Organizational	Nerc_Cip_R5	Is the responsible CIP Senior Manager authority delegation process documented and reviewed in a manner that identifies, assesses, and corrects deficiencies?
3422	Personnel	Nerc_Cip_R5	Is security awareness training given at least once each calendar quarter to users that have electronic or physical access to the BES cyber system ?

3423	Personnel	Nerc_Cip_R5	Does the Responsible Entity provide a cyber security awareness training that covers topics listed in CIP-004-5.1 Parts 2.1.1 through 2.1.9?
3424	Personnel	Nerc_Cip_R5	Does the Responsible Entity have a Cyber Security Training program as specified in CIP-004-5.1 R2 and is it offered at least once every 15 calendar months?
3425	Personnel	Nerc_Cip_R5	Are the results of personnel risk assessments documented, and are the risk assessments of contractor and service vendor personnel conducted pursuant to Standard CIP-004-5?
3426	Personnel	Nerc_Cip_R5	Is appropriate personnel access, physical or electronic, to designated storage locations for BES Cyber System Information verified at least once every 15 calendar months?
3427	Access Control	Nerc_Cip_R5	Is the Access Management Program documented, assessed, and if any deficiencies are found they are corrected?
3428	Personnel	Nerc_Cip_R5	Does the Responsible Entity verify user accounts at least every 15 calendar months?
3429	Communication Protection	Nerc_Cip_R5	Does the Responsible Entity have a documented interactive remote access policy that includes CIP-005-5 applicable requirements from Parts 2.1, 2.2, and 2.3?
3430	Physical Security	Nerc_Cip_R5	Are physical access logs retained for at least 90 calendar days and are logs related to reportable incidents kept in accordance with the requirements of CIP-006-5?
3431	Physical Security	Nerc_Cip_R5	Is there a maintenance and testing program performed at least every 24 calendar months to ensure that all physical security systems function properly?
3432	System Integrity	Nerc_Cip_R5	Does the Responsible Entity implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes from CIP-007-5 Table R3 - Malicious Code Prevention?
3433	System Integrity	Nerc_Cip_R5	Does the Responsible Entity implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes from CIP-007-5 Table R4 – Security Event Monitoring?
3434	System Integrity	Nerc_Cip_R5	Are user accounts reviewed at least annually to verify access privileges are in accordance with CIP-004-5 R4 requirements?
3435	System Integrity	Nerc_Cip_R5	Are user accounts implemented as approved by designated personnel per CIP-004-5 R4 requirements?
3436	Incident Response	Nerc_Cip_R5	Does the Responsible Entity implement and document processes from CIP-008-5 R1 for one or more Cyber Security Incident response plans and where deficiencies are identified, analyzed, and corrected?

3437	Incident Response	Nerc_Cip_R5	Has the Responsible Entity developed, documented and implemented a Cyber Security Incident response implementation and testing plan from CIP-008-5 R2 for one or more Cyber Security Incident response plans and where deficiencies are identified, analyzed, and corrected?
3438	Incident Response	Nerc_Cip_R5	Does the Responsible Entity maintain Cyber Security Incident response plans in a manner that reviews, updates and communicates roles and responsibilities?
3439	Continuity	Nerc_Cip_R5	Does the Responsible Entity have a documented recovery plan and a process that identifies and corrects deficiencies as described in CIP-009-5 R1?
3440	Continuity	Nerc_Cip_R5	Does the Responsible Entity implement one or more documented processes listed in CIP-009-5 R2 for a recovery plan implementation and testing? And are deficiencies identified and corrected?
3441	Continuity	Nerc_Cip_R5	Are updates to the recovery plans made and communicated to personnel responsible for the activation and implementation of the recovery plans within 60 calendar days of the change completion?
3442	Configuration Management	Nerc_Cip_R5	Does the organization monitor changes to the baseline configuration at least every 35 days?
2978	Access Control	NISTIR_7628	Does the organization control the use of personally owned and removable media in the Smart Grid system?
2979	Audit and Accountability	NISTIR_7628	Is the Smart Grid system configured to synchronize with internal Smart Grid system clocks on an organization-defined frequency using an organization-defined time source?
2980	Risk Management and Assessment	NISTIR_7628	Does the organization report the security state of the Smart Grid system to management authority according to company-defined policy?
2981	Configuration Management	NISTIR_7628	Does the organization analyze changes to the Smart Grid system for potential security impacts?
2982	Configuration Management	NISTIR_7628	Does the organization establish terms and conditions for installing any hardware, firmware, or software on Smart Grid system devices?
2983	Configuration Management	NISTIR_7628	Is there an inventory of the components of the Smart Grid system that documents the names or roles of the individuals responsible for administering those components?
2984	Configuration Management	NISTIR_7628	Are the factory default settings changed during maintenance?
2985	Continuity	NISTIR_7628	Are the continuity of operations security policy and the associated continuity of operations protection requirements developed, implemented, and reviewed according to company policy?

2986	Continuity	NISTIR_7628	Is the authorizing official or designated representative who reviews and approves the continuity of operations plan specified?
2987	Continuity	NISTIR_7628	Are individuals with continuity of operations roles and responsibilities identified?
2988	Continuity	NISTIR_7628	Does the organization train personnel in their continuity of operations roles and responsibilities?
2989	Information and Document Management	NISTIR_7628	Does the document management policy address the purpose of the document management security program as it relates to protecting the organization's personnel and assets?
2990	Information and Document Management	NISTIR_7628	Does the document management policy address the scope of the document management security program as it applies to all organizational staff and third-party contractors?
2991	Incident Response	NISTIR_7628	Does the organization train personnel in their incident response roles and responsibilities with respect to the Smart Grid system and receive refresher training defined by company policy?
2992	Communication Protection	NISTIR_7628	Are communications with Smart Grid information system components restricted to specific components in the Smart Grid information system? Also are communications with any non-Smart Grid system denied unless separated by a controlled logical/physical interface?
3804	Awareness and Training	NISTIR_7628_R1	Does the organization ensure that the awareness and training security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations?
3805	Audit and Accountability	NISTIR_7628_R1	Does the organization audit activities associated with configuration changes to the system?
3806	Security Assessment and Authorization	NISTIR_7628_R1	Does management commit to ensuring compliance with the organization's security assessment and authorization security policy and other regulatory requirements?
3807	Security Assessment and Authorization	NISTIR_7628_R1	Does a senior official sign and approve the security authorization to operate?
3808	Continuity	NISTIR_7628_R1	Are periodic reviews of compliance with the system security policy performed to ensure compliance with all applicable laws and regulatory requirements?
3809	Continuity	NISTIR_7628_R1	Does the continuity of operations security policy address protecting the organization's personnel and assets?
3810	Continuity	NISTIR_7628_R1	Has the organization identified circumstances that could inhibit the recovery of the system to a known, secure state and established procedures to provide compensating controls?

3811	Incident Response	NISTIR_7628_R1	Are the incident handling procedures integrated with continuity of operations procedures?
3812	Incident Response	NISTIR_7628_R1	Does the incident reporting procedure comply with applicable laws and regulations?
3813	Incident Response	NISTIR_7628_R1	Is the incident reporting procedure written so that it includes what is a reportable incident, granularity of information necessary, who receives the report, and the process for transmitting incident information?
3814	Maintenance	NISTIR_7628_R1	Does the organization sanitize system components to be serviced both at removal and re-installation?
3815	Physical and Environmental Protection	NISTIR_7628_R1	Does the organization ensure that investigation of and response to detected physical security incidents are part of the organization's incident response capability?
3816	Physical and Environmental Protection	NISTIR_7628_R1	Does the organization authorize, monitor, control, and document and maintain records for all system components entering and exiting the facility?
3817	Plans	NISTIR_7628_R1	Is a privacy impact assessment reviewed and approved by a management authority?
3818	Plans	NISTIR_7628_R1	Does the organizational planning and coordination of security related activities include both emergency and routine situations?
3819	Personnel	NISTIR_7628_R1	Does a formal accountability process comply with applicable regulatory requirements, policies, standards, and guidance?
3820	Risk Management and Assessment	NISTIR_7628_R1	Are system and information security impact levels specified and documented in the security plan for the system?
3821	Risk Management and Assessment	NISTIR_7628_R1	Does the organization review the system and information impact levels on a organizationally-defined frequency?
3822	Risk Management and Assessment	NISTIR_7628_R1	Are assessments conducted to determine risk impacts from unauthorized access, use, disclosure, disruption, modification, or destruction of information and systems?
3823	Risk Management and Assessment	NISTIR_7628_R1	Are risk assessments updated when significant changes occur to the system or on an organizationally-defined frequency?
3824	System and Services Acquisition	NISTIR_7628_R1	Are organization system acquisition contracts in compliance with applicable laws, regulations, and organization-defined security policies?
3825	System and Services Acquisition	NISTIR_7628_R1	Do the security engineering principles include a minimum standard for security and privacy?

3826	System and Services Acquisition	NISTIR_7628_R1	Do the security engineering principles include creation of a threat model for the system?
3827	System and Services Acquisition	NISTIR_7628_R1	Do the security engineering principles include updating product specifications to include mitigations for threats discovered during threat modeling?
3828	System and Services Acquisition	NISTIR_7628_R1	Do the security engineering principles include using secure coding practices?
3829	System and Services Acquisition	NISTIR_7628_R1	Do the security engineering principles include performance of a final security audit prior to authorization to operate in order to confirm adherence to security requirements?
3830	System and Services Acquisition	NISTIR_7628_R1	Do the security engineering principles include creation of a documented and tested security response plan in the event a vulnerability is discovered?
3831	System and Services Acquisition	NISTIR_7628_R1	Do the security engineering principles include creation of a documented and tested privacy response plan in the event a vulnerability is discovered?
3832	System and Services Acquisition	NISTIR_7628_R1	Do the security engineering principles include performance of a root cause analysis to understand the cause of identified vulnerabilities?
3833	System and Services Acquisition	NISTIR_7628_R1	Do the security engineering principles include ongoing software security training requirements for developers?
3834	System and Services Acquisition	NISTIR_7628_R1	Do the system developers/integrators perform testing of developed security code only on non-production systems?
3835	Communication Protection	NISTIR_7628_R1	Does the organization use cryptographic mechanisms to ensure information integrity?
3836	Communication Protection	NISTIR_7628_R1	Does the organization employ cryptographic mechanisms to prevent unauthorized disclosure of information during transmission?
3837	Communication Protection	NISTIR_7628_R1	Does the system employ secure methods for the establishment and management of cryptographic keys?
3838	Communication Protection	NISTIR_7628_R1	Are cryptography and other security functions (e.g. hashes, random number generators) that are required for use in smart grid information systems, NIST (FIPS) approved?
3839	Communication Protection	NISTIR_7628_R1	Has the organization developed a collaborative computing policy and do they update and review it on a defined frequency?
3840	Communication Protection	NISTIR_7628_R1	Does the organization document, monitor, and manage the use of mobile code within the system?
825	Policies	Nrc_571	Does the access control policy address the management of CDAs?
826	Policies	Nrc_571	Does the access control policy address the protection of password/key databases?

827	Policies	Nrc_571	Does the access control policy address the auditing of CDAs annually or immediately upon changes in personnel responsibilities or major changes in system configurations or functionality?
828	Access Control	Nrc_571	Are all user rights and privileges on the CDA assigned consistent with the user authorizations?
829	Access Control	Nrc_571	Are privileged functions for CDAs defined and documented?
830	Communication Protection	Nrc_571	Are there assigned authorizations for controlling the flow of information in near-real time, within CDAs and between interconnected systems?
831	Communication Protection	Nrc_571	Have the types of permissible and impermissible information flow between CDAs, security boundary devices, and boundaries been analyzed and addressed, and is the required level of authorization implemented as defined in the defensive strategy?
832	Communication Protection	Nrc_571	Are CDAs configured so user credentials are not transmitted in clear text, and is this documented in the access control policy?
833	Access Control	Nrc_571	Are the security functions restricted to the least number of users necessary?
834	Access Control	Nrc_571	Are physical notices installed for when a CDA cannot support system use notifications?
835	Access Control	Nrc_571	Are all end users required to report any suspicious activity to the Cybersecurity Program manager?
836	Access Control	Nrc_571	Are CDAs configured to allow users to directly initiate session lock mechanisms?
837	Physical Security	Nrc_571	Is the use of access controls documented, supervised, and reviewed?
838	Info Protection	Nrc_571	Is the hard and soft copy information in storage, in process, and in transmission labeled?
839	Access Control	Nrc_571	Are CDAs secured through media access control address locking, physical or electrical isolation, static tables, encryption, or monitoring?
840	Communication Protection	Nrc_571	Are protocols prohibited from initiating commands except within the same boundary?
841	Communication Protection	Nrc_571	Are protocols prohibited from initiating commands that could change the state of the CDA from a more secured posture to a less secured posture?
842	Portable/Mobile/Wireless	Nrc_571	Is wireless access only allowed through a boundary security control device and are wireless connections treated as outside of the security boundary?
843	Portable/Mobile/Wireless	Nrc_571	Is the use of wireless technologies for CDAs associated with safety-related and important-to-safety functions prohibited?
844	Portable/Mobile/Wireless	Nrc_571	Are mobile devices used only in one security level and mobile devices are not moved between security levels?

845	Communication Protection	Nrc_571	Are alternative controls or countermeasures implemented to protect the CDAs from cyber attack up to and including the design-basis threat (DBT) when proprietary protocols that create a lack of visibility are used?
846	Communication Protection	Nrc_571	Do you ensure that external systems cannot be accessed from higher levels, such as Levels 3 and 4?
847	Audit and Accountability	Nrc_571	Are CDAs prevented from purging audit event records on restart?
848	Audit and Accountability	Nrc_571	Are the justification and details for alternate compensating security controls documented for those instances in which a CDA cannot respond to audit processing failures?
849	Audit and Accountability	Nrc_571	Does the response to audit failures include using an external system to provide these capabilities?
850	Audit and Accountability	Nrc_571	Are methods of time synchronization used that do not introduce a vulnerability to cyber attack and/or common-mode failure?
851	Audit and Accountability	Nrc_571	Is audit information protected at the same level as the device sources?
852	Audit and Accountability	Nrc_571	Are CDAs and audit records protected against an individual falsely denying they performed a particular action?
853	System Protection	Nrc_571	Are CDAs configured to isolate security functions from nonsecurity functions including control of access to and integrity of the hardware, software, and firmware performing these security functions?
854	System Protection	Nrc_571	Are CDAs configured to use underlying hardware separation mechanisms to facilitate security function isolation?
855	Monitoring & Malware	Nrc_571	Are devices and ports locked via address locking to prevent MITM attacks and rogue devices from being added to the network?
856	Monitoring & Malware	Nrc_571	Is network access control used to prevent MITM attacks and rogue devices from being added to the network?
857	Monitoring & Malware	Nrc_571	Is the network monitored to detect MITM attacks and address resolution protocol poisoning?
858	Communication Protection	Nrc_571	Are CDAs configured to prohibit remote activation of collaborative computing (e.g., IM, video conferencing) and is there an indication of use to the local user?
859	Communication Protection	Nrc_571	Are systems that provide name/address resolution to CDAs configured to indicate the security status of child subspaces and, if the child supports secure resolution services, enabled verification of a chain of trust among parent and child domains?

860	Communication Protection	Nrc_571	Do CDAs fail in a known-state so that SSEP functions are not adversely impacted by the CDAs failure?
861	Account Management	Nrc_571	Do the identification and authentication policy and procedures ensure that the user identifier is issued to the intended party?
862	Account Management	Nrc_571	Do the identification and authentication policy and procedures require the disabling of user identifier after a maximum of 30 days of inactivity?
863	Account Management	Nrc_571	Do the identification and authentication policy and procedures require archiving of user identifiers?
864	Communication Protection	Nrc_571	Is secure domain-based authentication implemented?
865	Communication Protection	Nrc_571	Are domain controllers within the given security level they service?
866	Communication Protection	Nrc_571	Are domain controllers physically and logically secured?
867	Communication Protection	Nrc_571	Are domain trust relationships between domains that of different security levels prohibited?
868	Communication Protection	Nrc_571	Are domain authentication protocols prohibited from being passed between boundaries?
869	Communication Protection	Nrc_571	Is role-based access control used to restrict user privileges to only those required to perform the task?
870	Access Control	Nrc_571	Are passwords not found in a dictionary, and do they not contain predictable sequences of numbers or letters?
871	Access Control	Nrc_571	Are copies of master passwords stored in a secure location with limited access?
872	Access Control	Nrc_571	Is the authority to change master passwords limited to authorized personnel?
873	Physical Security	Nrc_571	Do adequate physical security controls exist requiring operators be both authorized and properly identified, and are they monitored so operator actions are audited and recorded?
874	Physical Security	Nrc_571	Is access to nonauthenticated human-machine interactions (NHMI) controlled so as to not hamper HMI while maintaining security of the NHMI and ensuring that access to the NHMI is limited to only authorized personnel?
875	Account Management	Nrc_571	Are SSEP functions not adversely affected by authentication, session lock, or session termination controls?

876	Audit and Accountability	Nrc_571	Is the auditing capability implemented on NHMIs to ensure that all operator activity is recorded and monitored by authorized and qualified personnel and are historical records maintained?
877	Account Management	Nrc_571	Is the user identifier disabled after a maximum of 30 days of inactivity?
878	Account Management	Nrc_571	Is the initial authenticator content defined? (Such as defining password length and composition, tokens, keys, and other means of authenticating)
879	Access Control	Nrc_571	Do CDA authentication mechanisms prevent information (e.g. debug information, system banners) that an attacker could use to compromise authentication mechanisms?
880	System Integrity	Nrc_571	Are the operating system and software patches documented to allow traceability, and is there verification that no extra services are reinstalled or reactivated?
881	Maintenance	Nrc_571	Are software components that are not required for the operation and maintenance removed or disabled before incorporating the CDA into the production environment?
882	Maintenance	Nrc_571	Are the components that were removed or disabled documented?
883	System Integrity	Nrc_571	all unused network device drivers
884	System Integrity	Nrc_571	unused peripherals
885	System Integrity	Nrc_571	messaging services
886	System Integrity	Nrc_571	servers or clients for unused services (e.g., ftp, smtp, telenet, outlook express)
887	System Integrity	Nrc_571	software compilers in all user workstations and servers except for development workstations and servers
888	System Integrity	Nrc_571	compilers for languages that are not used in the control system
889	System Integrity	Nrc_571	unused networking and communications protocols
890	System Integrity	Nrc_571	unused administrative utilities, diagnostics, network management, and system management functions
891	System Integrity	Nrc_571	backups of files, databases, and programs used only during system development
892	System Integrity	Nrc_571	all unused data and configuration files
893	System Integrity	Nrc_571	sample programs and scripts
894	System Integrity	Nrc_571	unused document processing utilities
895	System Integrity	Nrc_571	unused removable media support
896	System Integrity	Nrc_571	games
897	Communication Protection	Nrc_571	Does configuration of the host intrusion detection system (HIDS) include attributes to enable detection of cyber attacks up to and including the DBT?

898	Communication Protection	Nrc_571	Is the HIDS configured to log system and user account connections to alert security personnel if an abnormal situation occurs?
899	Communication Protection	Nrc_571	Is the HIDS configured so it does not adversely impact the CDA safety, security, and emergency preparedness functions?
900	Communication Protection	Nrc_571	Are the security logging storage devices configured as "append only" to prevent alteration of records on those storage devices?
901	Communication Protection	Nrc_571	Are rules updates and patches to the HIDS implemented as security issues identified?
902	Communication Protection	Nrc_571	Are the HIDS configuration documents secured to ensure that only authorized personnel may access them?
903	Communication Protection	Nrc_571	Are CDAs configured with the lowest privilege, data, commands, file, and account access?
904	Communication Protection	Nrc_571	Are system services configured to execute at the lowest privilege level possible for that service and is the configuration documented?
905	Configuration Management	Nrc_571	Is the changing or disabling of access to files and functions documented?
906	Access Control	Nrc_571	Is the BIOS password protected from unauthorized changes?
907	Access Control	Nrc_571	Are the mitigation measures documented when password protection of the BIOS is not technically feasible documented?
908	Access Control	Nrc_571	Are network devices used to limit access to and from specific zones?
909	System Integrity	Nrc_571	Is there documentation allowing the system administrators to reenable devices if the devices are disabled by software and document the configuration?
910	Configuration Management	Nrc_571	Is there verification and documentation that replacement devices are configured in a manner that is equal to or better than the original?
911	Monitoring & Malware	Nrc_571	Are vulnerability notifications processed within 4 hours of receipt of the vulnerability information?
912	Configuration Management	Nrc_571	Are updates or workarounds to the baseline authorized and documented before implementation?
913	Configuration Management	Nrc_571	Are received cybersecurity updates tested on a nonproduction system/device for validation before installing on production systems?
914	Configuration Management	Nrc_571	Does the nonproduction system/device accurately replicate the production CDA?
915	Info Protection	Nrc_571	Are automated mechanisms used to restrict access to media storage areas, audit access attempts, and grant accesses?

916	Info Protection	Nrc_571	Are digital and nondigital media protected during transport outside of controlled areas using defined security measures?
917	Info Protection	Nrc_571	Is the guidance in NIST SP 800-88 followed to sanitize CDA media?
918	Info Protection	Nrc_571	Is information destroyed by a method that precludes reconstruction by means available to the DBT adversaries?
919	Info Protection	Nrc_571	Is the CDA media requiring sanitization and the appropriate techniques and procedures to be used in the process identified?
920	Info Protection	Nrc_571	Is identified CDA media sanitized before disposal or release for reuse and is sanitization consistent?
921	Personnel	Nrc_571	Are exit interviews conducted promptly upon termination or transfer of an individual's employment?
922	Personnel	Nrc_571	Are appropriate personnel promptly informed of status change, transfer, or termination of an individual's employment?
923	Procedures	Nrc_571	neutralizing malicious activity?
924	Procedures	Nrc_571	secure monitoring and management of security mechanisms?
925	Procedures	Nrc_571	time synchronization for all security-related devices?
926	Procedures	Nrc_571	that the physical and logical security of the monitoring network matches or exceeds, and differs from, the systems or networks being monitored?
927	System Integrity	Nrc_571	Are there procedures for correcting security flaws in CDAs?
928	Procedures	Nrc_571	Are there procedures for performing vulnerability scans and assessments of the CDA to validate that the flaw has been eliminated before the CDA is put into production?
929	Portable/Mobile/Wireless	Nrc_571	Are users not allowed to introduce unauthorized removable media onto the CDAs?
930	Portable/Mobile/Wireless	Nrc_571	Are all media interfaces disabled that are not required for the operation of the CDA?
931	System Integrity	Nrc_571	Is the need, severity, methods, and timeframes for implementing security directives independently evaluated and determined?
932	System Integrity	Nrc_571	Are hardware access controls used to prevent unauthorized software changes?
933	System Integrity	Nrc_571	Are tamper evident packaging seals inspected on a regular basis?
934	Access Control	Nrc_571	Is information checked automatically for accuracy, completeness, validity, and authenticity as close to the point of origin as possible?
935	Access Control	Nrc_571	Are inputs passed to interpreters prescreened to prevent the content from being unintentionally interpreted as commands?

936	Policies & Procedures General	Nrc_571	Do the system maintenance policy and procedures cover assets located in all security boundaries?
937	Maintenance	Nrc_571	Are there mechanisms implemented to detect unauthorized command execution by an escorted individual OR are there personnel with required access authorization and knowledge necessary designated to supervise escorted personnel?
938	Physical Security	Nrc_571	Are officials designated to review and approve the access lists and authorization credentials?
939	Physical Security	Nrc_571	Is logical access controlled through the use of electronic devices and software?
940	Physical Security	Nrc_571	Is there adequate lighting for access monitoring devices?
941	Planning	Nrc_571	Does the defensive strategy include and identify the protective controls associated within each security level?
942	Planning	Nrc_571	Does the defensive model identify the logical boundaries for data transfer and associated communication protocols?
943	Planning	Nrc_571	Does the defensive model define the level of connectivity permitted between levels and individual CDAs?
944	Planning	Nrc_571	Are the elements of the defensive strategy incorporated into CDAs?
945	Planning	Nrc_571	Are the security controls applied commensurate with the risk associated to perform the function required?
946	Defense in Depth	Nrc_571	Is the highest degree of cybersecurity protection allocated to CDAs that carry out safety, important to safety, and security functions, and are they protected from lower defensive levels?
947	Defense in Depth	Nrc_571	Is remote access to CDAs located in the highest defensive level prevented?
948	Defense in Depth	Nrc_571	Is spoofing of addresses from one security level to another prevented?
949	Defense in Depth	Nrc_571	Is only one-way data flow from Level 4 to Level 3 and from Level 3 to Level 2 allowed?
950	Defense in Depth	Nrc_571	Is the initiation of communications from digital assets at lower security levels to digital assets at higher security levels prohibited?
951	Defense in Depth	Nrc_571	Is bi-directional communication only allowed between CDAs in Level 4 within a security Level 4?
952	Defense in Depth	Nrc_571	Do nonsafety systems that have bi-directional communication to safety systems have the same level of protection as the safety systems?
953	Defense in Depth	Nrc_571	Does one-way data flow from one level to other levels only occur through a device that enforces the security policy between each level and detects, prevents, delays, mitigates, and recovers from a cyber attack coming from the lower security level?

954	Defense in Depth	Nrc_571	Are data, software, firmware, and devices moved from lower levels of security to higher levels of security using a documented validation process or procedure that is trustworthy at or above the trust level of the device on which the data, code, information, or device that will be installed or connected?
955	Defense in Depth	Nrc_571	Are CDAs that provide safety, important-to-safety, security, or control functions allocated defensive Level 4 protection?
956	Defense in Depth	Nrc_571	Are CDAs that provide data acquisition functions allocated at least defensive Level 3 protection?
957	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels physically and logically secure and harden CDAs?
958	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels employ secure management communications and encryption in accordance with Appendix B to RG 5.71?
959	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels provide logging and alert capabilities?
960	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels provide intrusion detection and prevention capabilities?
961	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels detect and prevent malware from moving between boundaries?
962	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels have the ability to perform more than stateful inspection of the protocols used across the boundary?
963	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels deny traffic, except when explicitly authorized?
964	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels provide protocol, source, and destination filtering?
965	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels base blocking on source and destination address pairs, services, and ports?
966	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels do not permit either incoming or outgoing traffic by default?
967	Defense in Depth	Nrc_571	Are boundary control devices between higher and lower security levels managed through a direct connection to the firewall or through a dedicated interface?
968	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels not permit direct communication to the firewall from any of the managed interfaces?

969	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels record information on accepted and rejected connections, traffic monitoring, analysis, and intrusion detection?
970	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels forwards logs to a centralized logging server?
971	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels enforce destination authorization and restricts users by allowing them to reach only the CDAs necessary for their function?
972	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels record information flow for traffic monitoring, analysis, and intrusion detection?
973	Defense in Depth	Nrc_571	Are boundary control devices between higher and lower security levels deployed and maintained by authorized personnel trained in the technologies used?
974	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels permit acquisition and control networks to be severed from corporate networks in times of serious cyber incidents or when directed by authorized personnel?
975	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels contain a rule set that is evaluated, analyzed, and tested before deployment and routinely upon modification and updates to the operational software and firmware?
976	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels receive time synchronization from a trusted and dedicated source existing on the security network, attached directly to the CDA or via SNTP and a trusted key management process?
977	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels synchronize time with CDAs?
978	Defense in Depth	Nrc_571	Are boundary control devices between higher and lower security levels capable of forwarding logging information in a standard format to a secure logging server or use an external device?
979	Defense in Depth	Nrc_571	Are boundary control devices between higher and lower security levels logs routinely reviewed by personnel to detect malicious or anomalous activity?
980	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels contain a rule set that is updated quarterly?
981	Defense in Depth	Nrc_571	Do security boundary control devices between higher security levels and lower security levels use only physically and logically secured and hardened computing devices and flow control?

982	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels allow no information to be transferred directly from networks, systems, or CDAs at a lower security level to networks, systems, or CDAs at Level 4?
983	Defense in Depth	Nrc_571	Do boundary control devices between higher and lower security levels prevent viruses or other malicious or unwanted programs from propagating information between security levels?
984	Incident Response	Nrc_571	Do incident response procedures direct containment activities and provide for assisting operations personnel in conducting and operability determination?
985	Incident Response	Nrc_571	Do incident response procedures provide for isolating the affected CDA with approval by shift superintendent operations and verifying that surrounding or interconnected CDAs, networks, and support systems are not contaminated, degraded, or compromised?
986	Incident Response	Nrc_571	Do eradication activities identify the attack and the compromised pathway?
987	Incident Response	Nrc_571	Are incident response training exercises documented, and are personnel qualified and trained?
988	Incident Response	Nrc_571	Are drills of the incident response capability for CDAs tested and conducted at least annually?
989	Incident Response	Nrc_571	Are defined tests or drills or both used to update the incident response capability to maintain its effectiveness?
990	Incident Response	Nrc_571	Are the results of testing and drills documented?
991	Incident Response	Nrc_571	Are there incident response testing and drill procedures?
992	Incident Response	Nrc_571	Are automated mechanisms used to test or drill the incident response capability?
993	Incident Response	Nrc_571	Are announced and unannounced tests and drills conducted and documented?
994	Incident Response	Nrc_571	Is there an integrated cybersecurity incident response team (CSIRT)?
995	Incident Response	Nrc_571	In the event of an unplanned incident that reduces the number of required cybersecurity personnel, are other trained and qualified onsite cybersecurity personnel used, or are off-duty personnel called in within 2 hours from the time of discovery?
996	Incident Response	Nrc_571	Is the team provided with the technical skills and authority to effectively respond to a potential cybersecurity event?
997	Incident Response	Nrc_571	Are the processes, procedures, and controls documented that the team will employ upon the discovery or identification of a potential or actual cybersecurity attack?
998	Incident Response	Nrc_571	Is the identification of what constitutes a cybersecurity incident defined and documented?

999	Incident Response	Nrc_571	Is the identification of threat level classification for incidents defined and documented?
1000	Incident Response	Nrc_571	Is the description of actions to be taken for each component of the Incident Response & Recovery (IR&R) process defined and documented?
1001	Incident Response	Nrc_571	Is the description of individual postulated classes or categories of incidents or attacks and indicators and potential or planned methods of mitigation defined and documented?
1002	Incident Response	Nrc_571	Is the identification of defensive strategies that would assist in identifying and containing a cyber attack defined and documented?
1003	Incident Response	Nrc_571	Is the description of the CSIRT incident notification process defined and documented?
1004	Incident Response	Nrc_571	Is the description of incident documentation requirements defined and documented?
1005	Incident Response	Nrc_571	Is the establishment of coordinated and secure communication methods to be used between local and remote CSIRT members and outside agencies defined and documented?
1006	Incident Response	Nrc_571	Is the description of response escalation requirements defined and documented?
1007	Incident Response	Nrc_571	Is the following incident data collected: incident title, date of incident, reliability of report, type of incident, entry point, perpetrator, type of system, hardware and software impacted, brief description of incident, impact on organization, measures to prevent recurrence, and references?
1008	Incident Response	Nrc_571	Does the CSIRT consist of individuals with knowledge and experience in information and digital system technology?
1009	Incident Response	Nrc_571	Does the CSIRT consist of individuals with knowledge and experience in nuclear facility operations, engineering, and safety?
1010	Incident Response	Nrc_571	Does the CSIRT consist of individuals with knowledge and experience in physical and operational security?
1011	Incident Response	Nrc_571	Are the competent and trained incident response support personnel available year round, 24 hours per day to offer advice and assistance?
1012	Plans	Nrc_571	Does the incident response plan define the resources and management support needed to effectively maintain and mature an incident response capability?
1013	Plans	Nrc_571	Is the incident response plan reviewed and approved by the Cybersecurity Program Sponsor?
1014	Continuity	Nrc_571	the required response to events or conditions that activate the recovery plan?

1015	Continuity	Nrc_571	procedures for operating the CDAs in manual mode, when external electronic connections are severed, until secure conditions can be restored?
1016	Continuity	Nrc_571	processes and procedures for the backup and secure storage of information?
1017	Continuity	Nrc_571	complete and up-to-date logical diagrams depicting network connectivity?
1018	Continuity	Nrc_571	Does it contain current configuration information for components?
1019	Continuity	Nrc_571	Does it contain a list of personnel authorized for physical and cyber access to the CDA?
1020	Continuity	Nrc_571	a communication procedure and list of personnel to contact in the case of an emergency?
1021	Continuity	Nrc_571	documented requirements for the replacement of components?
1022	Continuity	Nrc_571	Does the contingency plan maintain the SSEP functions by developing and disseminating roles, responsibilities, and assigned individuals with contact information?
1023	Continuity	Nrc_571	Does the contingency plan maintain the SSEP functions by defining activities associated with determining the effects of CDAs after a compromise, disruption, or failure and restoring the CDAs?
1024	Continuity	Nrc_571	Is the contingency plan development coordinated with organizations responsible for related plans and requirements?
1025	Continuity	Nrc_571	Are the required resources and capacity maintained to ensure that necessary information processing, telecommunications, and environmental support exist during crisis situations?
1026	Continuity	Nrc_571	Are the resources needed to ensure that the capacity necessary for information processing, telecommunications, and environmental support exist during crisis situations documented?
1027	Continuity	Nrc_571	Do CDAs execute predetermined actions in the event of a loss of processing within a CDA or a loss of communication with operational facilities?
1028	Continuity	Nrc_571	Is recovery and reconstitution of CDAs included in contingency plan testing?
1029	Continuity	Nrc_571	Are alternate controls established and documented for when the contingency plan cannot be tested or exercised on production CDAs?
1030	Continuity	Nrc_571	Are scheduled and unscheduled system maintenance activities used as an opportunity to test or exercise the contingency plan?
1031	Continuity	Nrc_571	Are personnel trained in their contingency roles and responsibilities with respect to the CDAs?

1032	Continuity	Nrc_571	Is refresher training provided at least annually or consistent with the overall contingency program, whichever period is shorter?
1033	Continuity	Nrc_571	Are there training procedures, and are training records of individuals documented?
1034	Continuity	Nrc_571	Are training drills used to familiarize contingency personnel with the facility, CDAs, and available resources and in evaluating the site's capabilities to support contingency operations?
1035	Continuity	Nrc_571	Are realistic test/drill scenarios and environments used that effectively stress the CDAs?
1036	Continuity	Nrc_571	Is the timeframe established and documented when data or the CDA must be restored and the frequency at which critical data and configurations are changing?
1037	Continuity	Nrc_571	Are CDAs recovered and reconstituted to a known secure state following a disruption or failure? (Which may include regression testing)
1038	Training	Nrc_571	Are individuals trained to a level of cybersecurity knowledge appropriate to their assigned responsibilities?
1039	Training	Nrc_571	Are the requirements for cybersecurity awareness implemented and documented ?
1040	Training	Nrc_571	Is the content of cybersecurity training based on assigned roles and responsibilities?
1041	Training	Nrc_571	Is the content of cybersecurity training based on specific requirements identified by the defensive strategy?
1042	Training	Nrc_571	Is the content of cybersecurity training based on CDAs to which personnel have authorized access?
1043	Training	Nrc_571	Does the cybersecurity awareness training address the site-specific objectives, management expectations, programmatic authority, roles and responsibilities, policies, procedures, and consequences for noncompliance with the cybersecurity program?
1044	Training	Nrc_571	Does the cybersecurity awareness training address the general attack methodologies, appropriate, and inappropriate cybersecurity practices?
1045	Training	Nrc_571	Does the cybersecurity awareness training address unusually heavy network traffic?
1046	Training	Nrc_571	Does the cybersecurity awareness training address out of disk space or significantly reduced free disk space?
1047	Training	Nrc_571	Does the cybersecurity awareness training address unusually high CPU usage?
1048	Training	Nrc_571	Does the cybersecurity awareness training address creation of new user accounts?
1049	Training	Nrc_571	Does the cybersecurity awareness training address attempted or actual use of administrator-level accounts?
1050	Training	Nrc_571	Does the cybersecurity awareness training address locked-out accounts?

1051	Training	Nrc_571	Does the cybersecurity awareness training address account in-use when the user is not at work?
1052	Training	Nrc_571	Does the cybersecurity awareness training address cleared log files?
1053	Training	Nrc_571	Does the cybersecurity awareness training address full log files with unusually large number of events?
1054	Training	Nrc_571	Does the cybersecurity awareness training address antivirus or IDS alerts?
1055	Training	Nrc_571	Does the cybersecurity awareness training address disabled antivirus software and other security controls?
1056	Training	Nrc_571	Does the cybersecurity awareness training address unexpected patch changes?
1057	Training	Nrc_571	Does the cybersecurity awareness training address machines connecting to outside IP addresses?
1058	Training	Nrc_571	Does the cybersecurity awareness training address requests for information about the system?
1059	Training	Nrc_571	Does the cybersecurity awareness training address unexpected changes in configuration settings?
1060	Training	Nrc_571	Does the cybersecurity awareness training address unexpected system shutdown?
1061	Training	Nrc_571	Does the cybersecurity awareness training address unusual activity from control devices?
1062	Training	Nrc_571	Does the cybersecurity awareness training address loss of signal from control devices?
1063	Training	Nrc_571	Does the cybersecurity awareness training address unusual equipment in secure areas?
1064	Training	Nrc_571	Does the cybersecurity awareness training address the contacts to whom to report suspicious activity, incidents, and violations of cybersecurity policies, procedures, or practices?
1065	Training	Nrc_571	Does the cybersecurity awareness training explain why access and control methods are required?
1066	Training	Nrc_571	Does the cybersecurity awareness training address the measures users can employ to reduce risks?
1067	Training	Nrc_571	Does the cybersecurity awareness training address the impact on the organization if the control methods are not incorporated?
1068	Training	Nrc_571	Is there a training program for personnel performing, verifying, or managing activities within the scope of the program to ensure that suitable proficiency is achieved and maintained?

1069	Training	Nrc_571	Do individuals that have cybersecurity responsibilities related to programs, processes, procedures, or individuals that are involved in the design, modification, and maintenance of CDAs, receive technical training?
1070	Training	Nrc_571	Is cybersecurity-related technical training provided to individuals before authorizing access to CDAs or performing assigned duties?
1071	Training	Nrc_571	Is cybersecurity-related technical training provided to individuals when required by policy or procedure changes and plant modifications?
1072	Training	Nrc_571	Is cybersecurity-related technical training provided to individuals annually or at an interval as defined by the organization, whichever is shorter?
1073	Training	Nrc_571	Is cybersecurity-related technical training provided to those individuals whose roles and responsibilities involve designing, installing, operating, maintaining, or administering CDAs or associated networks?
1074	Training	Nrc_571	Does cybersecurity-related technical training include specific cybersecurity and engineering procedures, practices, and technologies, including implementation methods and design requirements?
1075	Training	Nrc_571	Does cybersecurity-related technical training include general information on cyber vulnerabilities, potential consequences to CDAs and networks of successful cyber attacks, and cybersecurity risk reduction methods?
1076	Training	Nrc_571	Are system managers, cybersecurity specialists, system owners, network administrators, and other personnel having access to system-level software provided with security-related technical training to perform their assigned duties?
1077	Training	Nrc_571	Do individuals who have programmatic and procedural cybersecurity authority and require the necessary skills and knowledge to execute capabilities expected of a cybersecurity specialist receive specialized cybersecurity training?
1078	Training	Nrc_571	Are the requirements for advanced training for designated security experts or specialists?
1079	Training	Nrc_571	Does advanced training include achievement and maintenance of the necessary up-to-date skills and knowledge in core competencies of data security, operation system security, application security, network security, security controls, intrusion analysis, incident management and response, digital forensics, penetration testing, and plant system functionality and operations?
1080	Training	Nrc_571	Does advanced training include competency in the use of tools and techniques to physically and logically harden CDAs and networks?

1081	Training	Nrc_571	Does advanced training include the provision of cybersecurity guidance, assistance, and training for other staff members?
1082	Training	Nrc_571	Does advanced training include the review of programmatic and system-specific cybersecurity plans and practices?
1083	Training	Nrc_571	Does advanced training include the assessment of CDAs, networks, and assets for compliance with cybersecurity policies?
1084	Training	Nrc_571	Does advanced training include the design, acquisition, installation, operation, maintenance, or administration of security controls?
1085	Training	Nrc_571	Is there a cross-functional cybersecurity team (CST)?
1086	Training	Nrc_571	Is there a program to share expertise and varied domain knowledge between members of the CST?
1087	Training	Nrc_571	Does the CST include a member of the information technology staff, an instrumentation and control system engineer, a control system operator, a subject matter expert in cybersecurity, and a member of the management staff?
1088	Training	Nrc_571	Does the cybersecurity subject matter experts' skills include network architecture and design, security processes and practices, and secure infrastructure design and operation?
1089	Training	Nrc_571	Does the CST include the control system vendor or system integrator?
1090	Training	Nrc_571	Does the CST periodically report directly to a specified group?
1091	Training	Nrc_571	Does the security training describe the physical processes being controlled as well as the associated CDAs and security controls?
1092	Training	Nrc_571	Is there a feedback process for personnel and contractors to refine the cybersecurity program and address identified training gaps?
1093	Training	Nrc_571	Is contact with selected security groups maintained to remain informed of recommended security practices, techniques, and technologies and to share current security-related information?
1094	Organizational	Nrc_571	Is the "Cyber Security Sponsor" staffed with a member of senior site management?
1095	Organizational	Nrc_571	Does the "Cyber Security Sponsor" have overall responsibility and accountability for the cybersecurity program, and do they provide the resources required for the development, implementation, and sustenance of the cybersecurity program?
1097	Organizational	Nrc_571	provide oversight of the plant cybersecurity operations?
1098	Organizational	Nrc_571	function as a single point of contact for issues related to site cybersecurity?
1099	Organizational	Nrc_571	provide oversight and direction on issues regarding nuclear plant cybersecurity?
1100	Organizational	Nrc_571	initiate and coordinate CSIRT functions?

1101	Organizational	Nrc_571	coordinate with the NRC during cybersecurity events?
1102	Organizational	Nrc_571	oversee and approve the development and implementation of a cybersecurity plan?
1103	Organizational	Nrc_571	ensure and approve the development and operation of the cybersecurity education, awareness, and training program?
1104	Organizational	Nrc_571	oversee and approve the development and implementation of cybersecurity policies and procedures?
1106	Organizational	Nrc_571	protects CDAs from cyber threat?
1107	Organizational	Nrc_571	understand the cybersecurity implications surrounding the overall architecture of plant networks, control systems, safety systems, operating systems, hardware platforms, plant specific applications, and the services and protocols upon which those applications rely?
1108	Organizational	Nrc_571	perform cybersecurity evaluations of digital plant systems?
1109	Organizational	Nrc_571	Does the Cyber Security Specialist conduct security audits, network scans, and penetration tests against CDAs as necessary?
1110	Organizational	Nrc_571	conduct cybersecurity investigations involving compromise of CDAs?
1111	Organizational	Nrc_571	preserve evidence collected during cybersecurity investigations to prevent loss of evidentiary value?
1112	Organizational	Nrc_571	maintain expert skill and knowledge level in the area of cybersecurity?
1114	Organizational	Nrc_571	personnel have knowledge of cyber forensics and functions in accordance with the incident response plan?
1115	Organizational	Nrc_571	initiate emergency action when required to safeguard CDAs from compromise?
1116	Organizational	Nrc_571	assist with the eventual recovery of compromised systems?
1117	Organizational	Nrc_571	contain and mitigate incidents involving critical and other support systems?
1118	Organizational	Nrc_571	restore compromised CDAs?
1119	Configuration Management	Nrc_571	Do the baseline configurations include a current list of all components, configuration of peripherals, version releases of current software, and switch settings of machine components?
1120	Configuration Management	Nrc_571	Is the minimum physical and logical access defined for the modifications?
1121	Configuration Management	Nrc_571	Does the configuration management program address discovered deviations?
1122	Configuration Management	Nrc_571	Are white-list, black-list, and gray-list application control technologies used?

1123	Configuration Management	Nrc_571	Is there an automated inventory of the components of CDAs used to detect the addition of unauthorized components or devices into the environment, and does it disable access by such components or devices or notify designated officials?
1124	Configuration Management	Nrc_571	Is there an inventory of the components of CDAs that documents the names or roles of the individuals responsible for administering those components?
1125	System and Services Acquisition	Nrc_571	Are all tools used to perform cybersecurity tasks or SSEP functions required to undergo a commercial qualification process similar to that for software engineering tools that are used to develop digital instrumentation and control systems?
1126	System and Services Acquisition	Nrc_571	Do new acquisitions contain security design information, capabilities or both to implement security controls in Appendix B to RG 5.71?
1127	System and Services Acquisition	Nrc_571	Do the security capabilities include being cognizant of evolving cybersecurity threats and vulnerabilities?
1128	System and Services Acquisition	Nrc_571	Do the security capabilities include being cognizant of advancements in cybersecurity protective strategies and security controls?
1129	System and Services Acquisition	Nrc_571	Do the security capabilities include conducting analyses of the effects that each advancement could have on the security, safety, and operation of critical assets, systems, CDAs, and networks and implementing these advancements in a timely manner?
1130	System and Services Acquisition	Nrc_571	Do the security capabilities include replacing legacy systems as they reach end of life with systems that incorporate security capabilities?
1131	System and Services Acquisition	Nrc_571	Are timeframes established to minimize the time it takes to deploy new and more effective protective strategies and security controls?
1132	System Integrity	Nrc_571	Are weak, unproven, or nonstandard cryptographic modules identified and eliminated?
1133	System Integrity	Nrc_571	Are insecure network protocols for sensitive communications identified and eliminated?
1134	System Integrity	Nrc_571	Are insecure configuration files or options that act to control features of the application identified and eliminated?
1135	System Integrity	Nrc_571	Are inadequate or inappropriate use of access control mechanisms to control access to system resources identified and eliminated?
1136	System Integrity	Nrc_571	Are inappropriate privileges being granted to users, processes, or applications identified and eliminated?
1137	System Integrity	Nrc_571	Are weak authentication mechanisms identified and eliminated?
1138	System Integrity	Nrc_571	Are improperly or failing to validate input and output data identified and eliminated?

1139	System Integrity	Nrc_571	Are insecure or inadequate logging of system errors or security-related information identified and eliminated?
1140	System Integrity	Nrc_571	Are format string vulnerabilities identified and eliminated?
1141	System Integrity	Nrc_571	Are privilege escalation vulnerabilities identified and eliminated?
1142	System Integrity	Nrc_571	Are unsafe database transactions identified and eliminated?
1143	System Integrity	Nrc_571	Are unsafe use of native function calls identified and eliminated?
1144	System Integrity	Nrc_571	Are hidden functions and vulnerable features embedded in the code identified and eliminated?
1145	System Integrity	Nrc_571	Are implemented security features that increase the risk of security vulnerabilities, increase susceptibility to cyber attack, or reduce the reliability of design-basis functions identified and eliminated?
1146	System Integrity	Nrc_571	Is the use of unsupported or undocumented methods or functions identified and eliminated?
1147	System Integrity	Nrc_571	Is the use of undocumented code or malicious functions that might allow either unauthorized access or use of the system or the system to behave beyond the system requirements identified and eliminated?
1148	System and Services Acquisition	Nrc_571	Is there documentation of the system design transformed into code, database structures, and related machine executable representations?
1149	System and Services Acquisition	Nrc_571	Is there documentation of the communication configuration and setup?
1150	System and Services Acquisition	Nrc_571	Are the results of the developer's security testing conducted in accordance with Section 12.5 of RG 5.71 verified and validated?
1151	System and Services Acquisition	Nrc_571	Are CDA security devices, security controls, and software tested to ensure that they do not compromise the CDA or the operation of an interconnected CDA operation before installation?
1152	System and Services Acquisition	Nrc_571	Are CDAs tested to ensure they do not provide a pathway to compromise the CDA or other CDAs?
1153	System and Services Acquisition	Nrc_571	Are the security controls in Appendixes B and C to RG 5.71 implemented in accordance with the process described in Section 3.1.6 of Appendix A to RG 5.71?
1154	System and Services Acquisition	Nrc_571	Are the security controls tested for effectiveness, as described in Section 4.1.2 of Appendix A to RG 5.71?
1155	System and Services Acquisition	Nrc_571	Are vulnerability scans performed in accordance with Section 4.1.3 of Appendix A to RG 5.71 and Section 13.1 of this plan?

1156	System and Services Acquisition	Nrc_571	Are vulnerability scans performed against the CDA in its integrated state and correction, elimination, or discussion of discovered vulnerabilities?
1157	System and Services Acquisition	Nrc_571	Is the CDA installed and tested in the target environment?
1158	System and Services Acquisition	Nrc_571	Is there an acceptance review and test of the CDA security features?
1159	System and Services Acquisition	Nrc_571	Are the security controls implemented in accordance with Appendix B of RG 5.71?
1160	System and Services Acquisition	Nrc_571	Is the effectiveness of the security controls implemented in accordance with Appendix C verified?
1161	System and Services Acquisition	Nrc_571	Are the security design features developed to address the identified security requirements for the CDA documented?
1162	System and Services Acquisition	Nrc_571	Are the security controls implemented in accordance with Appendix B to 5.7.1?
1163	System and Services Acquisition	Nrc_571	Does the documentation include a description of the feature, its method of implementation, and any configurable options associated with the feature?
1164	System and Services Acquisition	Nrc_571	Is each security feature traceable to its corresponding security requirement?
1165	System and Services Acquisition	Nrc_571	Are the security reviews of the implemented design by the cybersecurity organization responsible for the protection of the critical assets/systems/networks?
1166	System and Services Acquisition	Nrc_571	Does the security review ensure that the security design configuration item transformations from the requirements implemented are correct, accurate, and complete?
1167	System and Services Acquisition	Nrc_571	Are annual audits of CDAs required to verify the security controls present during testing remain in place and are functioning correctly in the production system?
1168	System and Services Acquisition	Nrc_571	Are annual audits of CDAs required to verify CDAs are free from known vulnerabilities and security compromises and continue to provide information on the nature and extent of compromises?
1169	Monitoring & Malware	Nrc_571	Are SSEP functions not adversely impacted by the scanning process?
1170	Monitoring & Malware	Nrc_571	If SSEP functions are adversely impacted by the scanning process, are the CDAs removed from service or replicated before scanning is conducted, or is scanning scheduled to occur during planned CDA maintenance cycles?

1171	Monitoring & Malware	Nrc_571	Where the organization cannot conduct vulnerability scanning on a production CDA because of the potential for an adverse impact on SSEP functions, alternate controls are employed?
1172	Monitoring & Malware	Nrc_571	Are historic audit logs reviewed to determine if a vulnerability identified in the CDA has been previously exploited?
1173	Risk Management and Assessment	Nrc_571	Are protection and mitigation of risk achieved by implementing the defense-in-depth strategies discussed in Section 3.2 of RG 5.71?
1174	Risk Management and Assessment	Nrc_571	Are protection and mitigation of risk achieved by implementing the security controls described in Appendixes B and C to RG 5.71?
1175	Risk Management and Assessment	Nrc_571	Are protection and mitigation of risk achieved by implementing digital equipment and software cyber attack detection, prevention, and recovery techniques and tools to the systems, structures, and components within the scope of the rule?
1176	Risk Management and Assessment	Nrc_571	Are protection and mitigation of risk achieved by implementing Section 4 of Appendix A of RG 5.71?
1177	Risk Management and Assessment	Nrc_571	Is there detailed information on how these requirements are implemented to achieve the high assurance objectives of security controls specified in this plan?
1178	Risk Management and Assessment	Nrc_571	Is the detailed information available for NRC inspections and audits?
1179	Organizational	Nrc_571	Is the corrective action program criteria consistent with RG 5.71 for adverse conditions and the requirements for corrective action implemented and documented?
1584	Risk Management and Assessment	Tsa	Has a risk assessment been conducted to weigh the benefits of implementing wireless networking against the potential risks for exploitation?
1585	Risk Management and Assessment	Tsa	Has the need for enhanced networking control technologies for wireless networks been evaluated prior to implementation?
1828	Risk Management and Assessment	Tsa	Has an assessment of wireless networking risk been performed before implementation?
1	Policies & Procedures General	Universal	Are security policies and procedures implemented to define roles, responsibilities, behaviors, and practices of an overall security program?
2	Policies & Procedures General	Universal	Does the security team assign roles and responsibilities in accordance with the policies and confirm that processes are in place to protect company assets and critical information?
3	Policies & Procedures General	Universal	Do the security policies and procedures ensure coordination or integration with the physical security plan?

4	Policies & Procedures General	Universal	Do the security policies and procedures delineate how the organization implements its emergency response plan and coordinates efforts with law enforcement agencies, regulators, Internet service providers, and other relevant organizations in the event of a security incident?
5	Policies & Procedures General	Universal	Are the external suppliers and contractors that can impact system security held to the same security policies and procedures as the organization's own personnel?
6	Policies & Procedures General	Universal	Do the security policies and procedures of second and third-tier suppliers that can impact system security comply with the procuring organizations corporate cyber security policies and procedures?
7	Plans	Universal	Are there policies and procedures for the delivery and removal of system assets in the system security plan?
8	Policies & Procedures General	Universal	Are policies and procedures in place to enforce explicit rules and management expectations governing user installation of software?
9	Plans	Universal	Does the security plan define and communicate the specific roles and responsibilities in relation to various types of incidents?
10	Plans	Universal	Is the security plan regularly tested to validate the system objectives?
11	Policies & Procedures General	Universal	Does the organization manage system-related data for both electronic and paper data and manage access to the data based on formally assigned roles and responsibilities?
12	Policies & Procedures General	Universal	Are there policies and procedures detailing the handling of information and are they periodically reviewed and updated?
13	Policies & Procedures General	Universal	Are there policies and procedures for the classification of data, both electronic and paper media?
14	Policies & Procedures General	Universal	Do the data policies and procedures establish retention policies and procedures for both electronic and paper media?
15	Policies & Procedures General	Universal	Do the data policies and procedures address sharing, copying, transmittal, and distribution appropriate for the level of protection required?
16	Policies & Procedures General	Universal	Do the data policies and procedures establish access to the data based on formally assigned roles and responsibilities for the system?
17	Policies & Procedures General	Universal	Do the policies and procedures detail the retrieval of written and electronic records, equipment, and other media for the system in the overall information and document management policy?
18	Policies & Procedures General	Universal	Do the policies and procedures detail the destruction of written and electronic records, equipment, and other media for the system, without compromising the confidentiality of the data?

19	Policies & Procedures General	Universal	Are there policies and procedures to upgrade existing legacy control systems to include security mitigating measures commensurate with the organization's risk tolerance and the risk to the system and processes controlled?
20	Policies & Procedures General	Universal	Are maintenance authorization and approval policies and procedures documented?
21	Configuration Management	Universal	Are policies and procedures implemented to address the addition, removal, and disposal of all system equipment?
22	Policies & Procedures General	Universal	Are roles and responsibilities established that address the overlap and synergy between physical and system security risks?
23	Policies & Procedures General	Universal	Is there a list of personnel authorized to perform maintenance on the system?
24	Policies	Universal	System Security Policy
25	Policies	Universal	Planning Policy
26	Policies	Universal	Personnel Security Policy
27	Policies	Universal	Physical and Environmental Policy
28	Policies	Universal	System and Services Acquisition Policy
29	Policies	Universal	Configuration Management Policy
30	Policies	Universal	System and Communication Protection Policy
31	Policies	Universal	Information and Document Management Policy
32	Policies	Universal	Maintenance Policy
33	Policies	Universal	Awareness and Training Policy
34	Policies	Universal	Incident Response Policy
35	Policies	Universal	Media Protection Policy
36	Policies	Universal	System Control and Integrity Policy
37	Policies	Universal	Access Control Policy
38	Policies	Universal	Identification and Authentication Policy
39	Policies	Universal	Audit and Accountability Policy
40	Policies	Universal	Monitoring and Review Policy
41	Policies	Universal	Security Assessment Policy
42	Policies	Universal	Cryptographic Policy
43	Policies	Universal	Risk Assessment Policy
44	Policies	Universal	Does the system security policy address the purpose of the security program as it relates to protecting the organization's personnel and assets?

45	Policies	Universal	Does the system security policy address the scope of the security program as it applies to all organizational staff and third-party contractors?
46	Policies	Universal	Are there legal reviews of the retention policies to ensure compliance with all applicable laws and regulations?
47	Policies	Universal	Are periodic reviews of compliance with the system information and document security management policy performed to ensure compliance with any laws and regulatory requirements?
48	Procedures	Universal	Security Procedure
49	Procedures	Universal	Personnel Security Procedure
50	Procedures	Universal	Physical and Environmental Procedure
51	Procedures	Universal	System and Services Acquisition Procedure
52	Procedures	Universal	Configuration Management Procedure
53	Procedures	Universal	Strategic Planning Procedure
54	Procedures	Universal	System and Communication Protection Procedure
55	Procedures	Universal	Information and Document Management Procedure
56	Procedures	Universal	Maintenance Procedure
57	Procedures	Universal	Awareness and Training Procedure
58	Procedures	Universal	Incident Response Procedure
59	Procedures	Universal	Media Protection Procedure
60	Procedures	Universal	System Control and Integrity Procedure
61	Procedures	Universal	Access Control Procedure
62	Procedures	Universal	Identification and Authentication Procedure
63	Procedures	Universal	Audit and Accountability Procedure
64	Procedures	Universal	Monitoring and Review Procedure
65	Procedures	Universal	Risk Assessment Procedure
66	Procedures	Universal	Security Assessment Procedure
67	Policies & Procedures General	Universal	Are procedures established to remove external supplier physical and electronic access at the conclusion/termination of the contract in a timely manner?
68	Procedures	Universal	Does a process exist to monitor changes to the system and conduct security impact analyses to determine the effects of the changes?
69	Plans	Universal	Configuration Management Plan
70	Plans	Universal	Security Plan
71	Plans	Universal	Continuity of Operations Plan
72	Plans	Universal	Incident Response Plan

73	Plans	Universal	Security Program Plan
74	Plans	Universal	Critical Infrastructure Plan
75	Plans	Universal	Is the risk assessment plan updated annually or whenever significant changes occur to the system, the facilities where the system resides, or other conditions that may affect the security or accreditation status of the system?
76	Plans	Universal	Does the security plan align with the organization's enterprise architecture?
77	Plans	Universal	Does the security plan explicitly define the authorization boundary of the system?
78	Plans	Universal	Does the security plan describe the relationships with or connections to other systems?
79	Plans	Universal	Does the security plan provide an overview of the security requirements for the system?
80	Plans	Universal	Does the security plan describe the security controls in place or planned?
81	Plans	Universal	Is the authorizing official or designated representative who reviews and approves the system security plan specified?
82	Plans	Universal	Is the security plan for the system reviewed on a defined frequency, annually at a minimum?
83	Plans	Universal	Does the security plan limit data ports, physical access, specific data technology, impose additional physical and electronic inspections and physical separation requirements?
84	Plans	Universal	Is the security plan revised to address changes to the system/environment or problems identified during plan implementation or security control assessments?
85	Plans	Universal	Does the configuration management plan define the configuration items for the system?
86	Plans	Universal	Does the configuration management plan define when the configuration items are placed under configuration management?
87	Plans	Universal	Does the configuration management plan define the means for uniquely identifying configuration items throughout the system development life cycle?
88	Plans	Universal	Does the configuration management plan define the process for managing the configuration of the configuration items?
89	Continuity	Universal	Does the continuity of operations plan address the issue of maintaining or re-establishing production in case of an undesirable interruption for the system?
90	Continuity	Universal	Do designated officials review and approve the continuity of operations plan?

91	Continuity	Universal	Does the continuity of operations plan delineate that at the time of the disruption to normal system operations, the organization executes its incident response policies and procedures to place the system in a safe configuration and initiates the necessary notifications to regulatory authorities?
92	Continuity	Universal	Is the continuity of operations plan tested to determine its effectiveness, and are the results documented?
93	Continuity	Universal	Do the appropriate officials review the documented test results and initiate corrective actions if necessary?
94	Continuity	Universal	Is the continuity of operations plan tested at least annually, using organization-prescribed tests and exercises?
95	Continuity	Universal	Is the continuity of operations plan testing and exercises coordinated with the organizational elements responsible for related plans?
96	Continuity	Universal	Is the continuity of operations plan tested and exercised at the alternate processing site?
97	Continuity	Universal	Are exercises used to thoroughly and effectively test and exercise the continuity of operations plan?
98	Continuity	Universal	Is the continuity of operations plan reviewed at least annually and updated to address system, organizational, and technology changes or problems encountered during plan implementation, execution, or testing?
99	Plans	Universal	Are copies of the incident response plan distributed to active incident response personnel?
100	Plans	Universal	Is the incident response plan reviewed on a periodic frequency?
101	Plans	Universal	Is the incident response plan revised to address system/organizational/operational changes or problems encountered during plan implementation, execution, or testing?
102	Plans	Universal	Are incident response plan changes communicated to active incident response personnel?
103	Plans	Universal	Is the incident response investigation and analysis process developed, tested, deployed, and documented?
104	Plans	Universal	Are roles and responsibilities specified with respect to local law enforcement and/or other critical stakeholders in an internal and shared incident response investigation and analysis program?
105	Plans	Universal	Has a risk management plan been developed?
106	Plans	Universal	Does a senior official review and approve the risk management plan?

107	Plans	Universal	Is there a current plan of action and milestones for the system that documents the planned, implemented, and evaluated remedial actions to correct weaknesses or deficiencies noted during the assessment?
108	Plans	Universal	Is the plan of action reviewed at least annually?
109	Plans	Universal	Is there a process for ensuring that the action plan and milestones for the security program and the associated organizational systems are maintained?
110	Plans	Universal	Does the security plan provide sufficient information about the program management controls and common controls to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended?
111	Plans	Universal	Does the security program plan include roles, responsibilities, management commitment, coordination among organizational entities, and compliance?
112	Plans	Universal	Is the security plan approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations, organizational assets, individuals, and other organizations?
113	Plans	Universal	Is the organization-wide security plan reviewed on a defined frequency, at least annually?
114	Plans	Universal	Is the security plan revised to address organizational changes and problems identified during plan implementation or security control assessments?
115	Plans	Universal	Does the incident response plan provide a roadmap for implementing the incident response capability?
116	Plans	Universal	Does the incident response plan describe the structure and organization of the incident response capability?
117	Plans	Universal	Does the incident response plan provide a high-level approach for how the incident response capability fits into the overall organization?
118	Plans	Universal	Does the incident response plan meet the unique requirements of the organization's mission, function, size, and structure?
119	Plans	Universal	Does the incident response plan define reportable incidents?
120	Plans	Universal	Does the incident response plan provide metrics for measuring the incident response capability?
121	Plans	Universal	Are security issues addressed in the development, documentation, and updating of a critical infrastructure and key resources protection plan?
122	Plans	Universal	Is the investigation and analysis of system incidents included in the planning process?

123	Risk Management and Assessment	Universal	Are the security controls in the system assessed on a defined frequency, at least annually, to determine the extent the controls are implemented correctly, operating as intended, and producing the desired outcome?
124	Risk Management and Assessment	Universal	Is a security assessment report produced that documents the results of the assessment?
125	Risk Management and Assessment	Universal	Are periodic, unannounced, in-depth monitoring, penetration testing, and red team exercises included as part of the security control assessments?
126	Risk Management and Assessment	Universal	Are the system connections monitored on an ongoing basis verifying enforcement of documented security requirements?
127	Risk Management and Assessment	Universal	Are the security mechanisms in the system monitored on an ongoing basis? (audit, studies, analysis, etc.)
128	Risk Management and Assessment	Universal	Are the security mechanisms that are volatile or critical to protecting the system assessed at least annually?
129	Risk Management and Assessment	Universal	Are all noncritical or nonvolatile security mechanisms assessed at least once during the system's 3-year accreditation cycle for regulated systems?
130	Risk Management and Assessment	Universal	Is there an independent assessor or assessment team to monitor the security controls in the system on an ongoing basis?
131	Risk Management and Assessment	Universal	Are information and systems categorized in accordance with applicable management orders, policies, regulations, standards, and guidance?
132	Risk Management and Assessment	Universal	Are the security categorization results documented in the system security plan?
133	Risk Management and Assessment	Universal	Is the security categorization decision reviewed and approved by the authorizing official?
134	Risk Management and Assessment	Universal	Are potential security threats, vulnerabilities, and consequences identified, classified, prioritized, and analyzed using accepted methodologies?
135	Plans	Universal	Does the plan of action call out remedial security actions to mitigate risk to organizational operations and assets, individuals, other organizations?
136	Risk Management and Assessment	Universal	Is there a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations?
137	Risk Management and Assessment	Universal	Is the risk management strategy implemented consistently across the organization?
138	Organizational	Universal	Is there a defined framework of management leadership accountability that establishes roles and responsibilities to approve cybersecurity policy, assign security roles, and coordinate the implementation of cybersecurity?

139	Policies	Universal	Does sufficient authority and an appropriate level of funding exist to implement the security policy?
140	Organizational	Universal	Do contracts with external entities address security policies and procedures with business partners, third-party contractors, and outsourcing partners?
141	Organizational	Universal	Does the mission/business case planning include a determination of system security requirements?
142	Organizational	Universal	Does the capital planning and investment control process include the determination, documentation, and allocation of the resources required to protect the system?
143	Policies & Procedures General	Universal	Is the system managed using a system development life-cycle methodology that includes security considerations?
144	Risk Management and Assessment	Universal	Are risk-reduction mitigation measures planned and implemented, and the results monitored to ensure effectiveness of the risk management plan?
145	Organizational	Universal	Are a set of rules that describes the system users responsibilities and expected behavior established and made available?
146	Organizational	Universal	Are security-related activities affecting the system planned and coordinated before conducting such activities to reduce the impact on organizational operations, organizational assets, or individuals?
147	Organizational	Universal	Does the system design and implementation process define the security roles and responsibilities for the users of the system?
148	Organizational	Universal	Are individuals with system security roles and responsibilities identified?
149	Organizational	Universal	Does the security program implement continuous improvement practices to ensure that industry lessons learned and best practices are incorporated into system security policies and procedures?
150	Policies	Universal	Is there a process for monitoring and reviewing the performance of cybersecurity policy?
151	Organizational	Universal	Are industry best practices incorporated into the security program?
152	Organizational	Universal	Is the system authorized before being placed into operations and is the authorization updated on a defined frequency or when significant changes occur?
153	Organizational	Universal	Does a senior official sign and approve the security accreditation?
154	Organizational	Universal	Is an independent certification agent or certification team used to assess the security mechanisms in the system?
155	Organizational	Universal	Does the authorizing official decide on the required level of certifier independence based on the criticality and sensitivity of the system and the ultimate risk to operations and organizational assets and individuals?

156	Organizational	Universal	Does the authorizing official determine if the level of certifier independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision?
157	Organizational	Universal	Has the authorizing official consulted with representatives of the appropriate regulatory bodies, the senior agency information security officer, and the chief information officer to fully discuss the implications of any decisions on certifier independence.
158	Organizational	Universal	Is a senior security officer appointed with the mission and resources to coordinate, develop, implement, and maintain an organization-wide security program?
159	Organizational	Universal	Do all capital planning and investment requests include the resources needed to implement the security program, and are exceptions documented?
160	Organizational	Universal	Is a business case used to record the resources required?
161	Organizational	Universal	Are security resources available for expenditure as planned and approved?
162	Monitoring & Malware	Universal	Are the results of security measures of performance monitored and reported?
163	Organizational	Universal	Is the security state of organizational systems managed through security authorization processes?
164	Organizational	Universal	Is the security authorization processes fully integrated into an organization-wide risk management strategy?
165	Organizational	Universal	Are the mission/business processes defined with consideration for security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the nation?
166	Organizational	Universal	Are protection needs arising from the defined mission/business processes determined and the processes revised as necessary until an achievable set of protection needs is obtained?
167	Organizational	Universal	Is the independent certification agent or certification team an individual or group capable of conducting an impartial assessment of an organizational control system?
168	Organizational	Universal	Is the system owner prevented from being directly involved in the contracting process and from unduly influencing the independence of the certification agent or certification team conducting the assessment of the security mechanisms in the system?

169	Organizational	Universal	In special situations, is the independence of the certification process achieved by ensuring the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, consistency, and veracity of the results?
170	Personnel	Universal	Is a risk designation assigned to all positions and are screening criteria established for individuals filling those positions?
171	Personnel	Universal	Are position risk designations periodically reviewed and revised?
172	Personnel	Universal	Are individuals requiring access screened before access is authorized?
173	Personnel	Universal	Are individuals with access rescreened based on a defined list of conditions and frequency?
174	Personnel	Universal	Is the logical and physical access to systems and facilities revoked for terminated employees?
175	Personnel	Universal	Does the organization ensure all organization-owned property is returned for terminated employees?
176	Personnel	Universal	Are documents and data files in the terminated employee's possession transferred to new authorized owners?
177	Personnel	Universal	Are all required controls for employees terminated for cause completed within 24 hours?
178	Personnel	Universal	Are automated processes used to revoke access permissions for terminated employees?
179	Personnel	Universal	Are electronic and physical access permissions reviewed when individuals are reassigned or transferred?
180	Personnel	Universal	Are electronic and physical access permissions reviewed within 7 days when individuals are reassigned or transferred?
181	Policies & Procedures General	Universal	Are security controls for third-party personnel enforced, and is service provider behavior and compliance monitored?
182	Personnel	Universal	Does a formal accountability process exist that clearly documents potential disciplinary actions for failing to comply?
183	Personnel	Universal	Are employees and contractors provided with complete job descriptions including detailed expectations of conduct, duties, terms and conditions of employment, legal rights, and responsibilities?
184	Personnel	Universal	Do employees and contractors acknowledge understanding of the job description by signature?

185	Personnel	Universal	Are periodic reviews of physical and electronic access conducted to validate terminated account access was removed?
186	Training	Universal	Is training on the implementation of the system security plan included for employees, contractors, and stakeholders?
187	Training	Universal	Is basic security awareness training provided to all system users before authorizing access to the system, when required by system changes and at least annually thereafter?
188	Training	Universal	Is the effectiveness of security awareness training reviewed once a year at a minimum?
189	Training	Universal	Are all system design and procedure changes reviewed for inclusion in the organization security awareness training?
190	Training	Universal	Are practical exercises included in the security awareness training that simulate actual cyber attacks?
191	Training	Universal	Are system security roles and responsibilities defined and documented throughout the system development life cycle, and are the individuals who have these roles and responsibilities identified and trained?
192	Training	Universal	Is security-related technical training provided before authorizing access to the system or performing assigned duties, when required by system changes and on an periodic basis?
193	Training	Universal	Are individual system security training activities documented, maintained, and monitored?
194	Training	Universal	Is contact with security groups and associations established and maintained?
195	Training	Universal	Is the knowledge of personnel on security policies and procedures based on their roles and responsibilities documented and tested?
196	Training	Universal	Is refresher training provided on a defined frequency, at least annually?
197	Training	Universal	Are simulated events incorporated into continuity of operations training to facilitate effective response by personnel in crisis situations?
198	Training	Universal	Are automated mechanisms used to provide a thorough and realistic system training environment?
199	Account Management	Universal	Are system accounts identified by account type and managed?
200	Account Management	Universal	Do system accounts have conditions for group membership?

201	Account Management	Universal	Are the access rights and privileges specified, and are authorized users identified for system accounts?
202	Account Management	Universal	Are appropriate approvals required for requests to establish accounts?
203	Account Management	Universal	Are system accounts authorized, established, activated, modified, disabled, and removed?
204	Account Management	Universal	Are system accounts reviewed on a defined frequency?
205	Account Management	Universal	Is the use of guest/anonymous accounts specifically authorized and monitored?
206	Account Management	Universal	Are account managers notified when system users are terminated, transferred, or system usage or need-to-know/need-to-share changes?
207	Account Management	Universal	Is access to the system granted based on a valid need-to-know or need-to-share as determined by official duties and satisfying all security criteria?
208	Account Management	Universal	Are automated mechanisms such as active directory used to support the management of system accounts?
209	Account Management	Universal	Does the system automatically terminate temporary and emergency accounts after a defined time period for each type of account?
210	Account Management	Universal	Does the system automatically disable inactive accounts after a defined time period?
211	Account Management	Universal	Does the system automatically audit account creation, modification, disabling, and termination actions and notify appropriate individuals?
212	Account Management	Universal	Are currently active system accounts reviewed on a defined frequency to verify that temporary accounts and accounts of terminated or transferred users have been deactivated?
213	Account Management	Universal	Are user account names different than email user accounts?
214	Account Management	Universal	Is there an official assigned to authorize a user or device identifier?
215	Account Management	Universal	Are identifiers selected that uniquely identify an individual or device?
216	Account Management	Universal	Are the user identifiers assigned to the intended party or the device identifier to the intended device?

217	Account Management	Universal	Are previous user or device identifiers archived?
218	Account Management	Universal	Is there a mechanism in place to verify the identity whenever an authenticator (password, token) is created, distributed, or modified?
219	Account Management	Universal	Is the initial authenticator content for organization-defined authenticators established?
220	Account Management	Universal	Do authenticators have sufficient strength of mechanism for their intended use?
221	Account Management	Universal	Are there administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators? (e.g., passwords, tokens, cards, etc.)
222	Account Management	Universal	Is the default content of authenticators changed on system installation?
223	Account Management	Universal	Are there minimum and maximum lifetime restrictions and reuse conditions for authenticators?
224	Account Management	Universal	Are authenticators changed or refreshed periodically as appropriate for authenticator type?
225	Account Management	Universal	Is authenticator content protected from unauthorized disclosure and modification? (i.e., not transmitting over email as open text)
226	Account Management	Universal	Are users required to take, and devices implement, specific measures to safeguard authenticators?
227	Account Management	Universal	Are certificates validated for PKI-based authentication by constructing a certification path with status information to an accepted trust anchor?
228	Account Management	Universal	Is the registration process to receive a user authenticator carried out in person before a designated registration authority?
229	Account Management	Universal	Are automated tools used to determine if authenticators are sufficiently strong to resist attacks intended to discover or otherwise compromise the authenticators?
230	Account Management	Universal	Are unique authenticators required to be provided by vendors and manufacturers of system components?
231	Account Management	Universal	Is there a division of responsibilities and separation of duties of individuals to eliminate conflicts of interest?
232	Account Management	Universal	Is the separation of duties implemented through assigned system access authorizations?
233	Access Control	Universal	Is the concept of least privilege used to accomplish assigned tasks?

234	Account Management	Universal	Is access to a defined list of security functions and security-relevant information explicitly authorized?
235	Account Management	Universal	Are users of system accounts with access to a defined list of security functions or security-relevant information required to use nonprivileged accounts when accessing other system functions?
236	Account Management	Universal	Is network access to defined privileged commands authorized only for compelling operational needs and is the rationale documented?
237	Account Management	Universal	Does the system enforce authorized access to the corresponding private key for PKI-based authentication?
238	Account Management	Universal	Does the system map the authenticated identity to the user account for PKI-based authentication?
239	Access Control	Universal	Are periodic reviews conducted of existing authorized physical and electronic access permissions to ensure they are current?
240	Access Control	Universal	Are appropriate agreements finalized before access is granted, including for third parties and contractors?
241	Access Control	Universal	Are access agreements periodically reviewed and updated?
242	Access Control	Universal	Are security measures in place to restrict information input to the system to authorized personnel only?
243	Access Control	Universal	Has a signed acknowledgement been obtained from users indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to the system?
244	Access Control	Universal	Are explicit restrictions on the use of social networking sites, posting information on commercial Web sites, and sharing system account information included in the rules of behavior?
245	Access Control	Universal	Do electronic monitoring mechanisms alert system personnel when unauthorized access or an emergency occurs?
246	Access Control	Universal	Is public access to the system denied?
247	Access Control	Universal	Is business IT and general corporation access to the system NOT permitted?
248	Access Control	Universal	Does the system enforce assigned authorizations for controlling electronic access to the system?
249	Access Control	Universal	Are access control policies and associated access mechanisms to control access to the system?

250	Access Control	Universal	Does the system enforce defined nondiscretionary access control policies over a defined set of users and resources that specify the access control information employed and the required relationships among the access control information to permit access?
251	Access Control	Universal	Does the system prevent access to security-relevant information (except during secure nonoperable system states)?
252	Access Control	Universal	Does the system uniquely identify and authenticate organizational users?
253	Access Control	Universal	Does the system employ multifactor authentication for remote access?
254	Access Control	Universal	Does the system employ multifactor authentication for network access and for access to privileged accounts?
255	Access Control	Universal	Does the system employ multifactor authentication for local system access for all users?
256	Access Control	Universal	Are specific user actions that can be performed on the system without identification or authentication identified and documented?
257	Access Control	Universal	Are actions to be performed without identification and authentication permitted only to the extent necessary to accomplish mission objectives?
258	Access Control	Universal	Is a device verified against a pre-defined list of authorized devices before a connection is established? (e.g., Active Directory policy or firewall rules.)
259	Access Control	Universal	Does the system authenticate devices before establishing remote network connections using bi-directional authentication between devices that are cryptographically based?
260	Access Control	Universal	Does the system authenticate devices before establishing network connections, using bidirectional authentication between devices that are cryptographically based?
261	Access Control	Universal	Do the authentication mechanisms obscure feedback of authentication information during the authentication process (i.e., does not return any system specific information)?
262	Access Control	Universal	Does the system employ authentication methods that meet the requirements of applicable policies, standards, and guidance for authentication to a cryptographic module?
263	Access Control	Universal	If your authentication encryption module fails can you still authenticate without creating a denial of service that impacts operational performance of system?
264	Access Control	Universal	Are there policies and procedures concerning the generation and use of passwords?
265	Access Control	Universal	Do the password policies stipulate rules of complexity, based on the criticality level of the systems to be accessed?

266	Access Control	Universal	Does system deployment require two-factor authentication or comparable compensating measures?
267	Access Control	Universal	Does the system display an approved system use notification message or banner before granting access to the system?
268	Access Control	Universal	Does the banner provide privacy and security notices consistent with applicable policies, regulations, standards, and guidance and state that: (a) users are accessing a private or government system; (b) system usage may be monitored, recorded, and subject to audit; (c) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (d) use of the system indicates consent to monitoring and recording?
269	Access Control	Universal	Does the system retain the notification message or banner on the screen until users take explicit actions to log on to or further access the system?
270	Access Control	Universal	Does the system: (a) display the system use information before granting further access; (b) ensure that any references to monitoring, recording, or auditing are consistent with privacy accommodations for such systems that generally prohibit those activities; and (c) include a description of the authorized uses of the system?
271	Access Control	Universal	Are the number of concurrent sessions for any user limited?
272	Access Control	Universal	Does the system log both successful and unsuccessful logon attempts?
273	Access Control	Universal	Does the system notify the user upon successful logon of the number of unsuccessful logon attempts since the last successful logon?
274	Access Control	Universal	Does the system notify the user/admin of unsuccessful logon attempts?
275	Access Control	Universal	Does the system capture security-related changes to the user's account?
276	Access Control	Universal	Does the system enforce a limit of a defined number of consecutive invalid access attempts by a user during a defined time period?
277	Access Control	Universal	Does the system automatically lock the account/node for a defined time period, delaying the next login prompt when the maximum number of unsuccessful attempts are exceeded?
278	Access Control	Universal	Does the system automatically lock the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded?
279	Access Control	Universal	Does the system prevent further access to the system by initiating a session lock after a defined time period of inactivity or a user initiated session lock?
280	Access Control	Universal	Does the system retain the session lock until the user re-establishes access using appropriate identification and authentication procedures?

281	Access Control	Universal	Does the system session lock mechanism place a publicly viewable pattern onto the associated display hiding what was previously visible on the screen?
282	Remote Access Control	Universal	Does the system terminate a network connection at the end of a session or after a defined time period of inactivity?
283	Remote Access Control	Universal	Is automatic session termination applied to local and remote sessions?
284	Remote Access Control	Universal	Does the system terminate a network connection at the end of a session or after a period of inactivity?
285	Remote Access Control	Universal	Are allowed methods of remote access to the system documented?
286	Remote Access Control	Universal	Are there usage restrictions and implementation guidance for each allowed remote access method?
287	Remote Access Control	Universal	Does remote access to the network require authentication prior to system connection?
288	Remote Access Control	Universal	Are the requirements for remote connections to the system enforced?
289	Remote Access Control	Universal	Are all the methods of remote access to the system authorized, monitored, and managed?
290	Remote Access Control	Universal	Are automated mechanisms used to facilitate the monitoring and control of remote access methods?
291	Remote Access Control	Universal	Is cryptography used to protect the confidentiality and integrity of remote access sessions?
292	Remote Access Control	Universal	Does the system route all remote accesses through a limited number of managed access control points?
293	Remote Access Control	Universal	Is remote access for privileged commands and security-relevant information authorized only for compelling operational needs and is the rationale for such access documented?
294	Remote Access Control	Universal	Is Bluetooth wireless networking capability disabled except for explicitly identified components in support of specific operational requirements?
295	Remote Access Control	Universal	Are there mechanisms in the design and implementation of the system to restrict access to the system from the enterprise network? (firewall, DMZ, VPN)
296	Remote Access Control	Universal	Are the terms and conditions established for authorized individuals to access the system from an external system?

297	Remote Access Control	Universal	Are the terms and conditions established for authorized individuals to process, store, and transmit organization-controlled information using an external system?
298	Remote Access Control	Universal	Are authorized individuals prohibited from using an external system to access the system or to process, store, or transmit organization-controlled information except in situations where the organization: (a) can verify the implementation of required security controls on the external system as specified in the organization's security policy and security plan, or (b) has approved system connection or processing agreements with the organizational entity hosting the external system?
299	Remote Access Control	Universal	Are restrictions imposed on authorized individuals with regard to the use of organization-controlled removable media on external systems?
300	Portable/Mobile/Wireless	Universal	Are usage restrictions and implementation guidance established for organization-controlled mobile devices?
301	Portable/Mobile/Wireless	Universal	Is mobile device connection to the system authorized?
302	Portable/Mobile/Wireless	Universal	Are requirements for mobile device connection to the system enforced?
303	Portable/Mobile/Wireless	Universal	Is the capability for automatic execution of code on removable media disabled?
304	Portable/Mobile/Wireless	Universal	Are specially configured mobile devices issued to individuals traveling to locations of significant risk per policies and procedures?
305	Portable/Mobile/Wireless	Universal	Are specified measures applied to mobile devices returning from locations of significant risk per policies and procedures?
306	Portable/Mobile/Wireless	Universal	Is the use of writable, removable media restricted on the system?
307	Portable/Mobile/Wireless	Universal	Is the use of personally owned, removable media prohibited on the system?
308	Portable/Mobile/Wireless	Universal	Is the use of removable media with no identifiable owner prohibited on the system?
309	Portable/Mobile/Wireless	Universal	Are usage restrictions and implementation guidance established for mobile code technologies based on the potential to cause damage to the system if used maliciously? (Java, JavaScript, ActiveX, Postscript, etc.)
310	Portable/Mobile/Wireless	Universal	Is the use of mobile code documented, monitored, and managed? (Java, JavaScript, ActiveX, Postscript, etc.)

311	Portable/Mobile/Wireless	Universal	Do appropriate officials authorize the use of mobile code?
312	Portable/Mobile/Wireless	Universal	Does the system implement detection and inspection mechanisms to identify unauthorized mobile code and take corrective actions?
313	Portable/Mobile/Wireless	Universal	Are there use restrictions and implementation guidance for wireless technologies?
314	Portable/Mobile/Wireless	Universal	Is wireless access to the system authorized, monitored, and managed?
315	Portable/Mobile/Wireless	Universal	Is authentication and encryption used to protect wireless access to the system and the latency induced does NOT degrade the operational performance of the system?
316	Portable/Mobile/Wireless	Universal	Is the system scanned for unauthorized wireless access points at a specified frequency, and is appropriate action taken if such access points are discovered?
317	Portable/Mobile/Wireless	Universal	Is there a thorough scan for unauthorized wireless access points in facilities containing high-impact systems?
318	Portable/Mobile/Wireless	Universal	Does the system protect wireless access using authentication and encryption?
319	Portable/Mobile/Wireless	Universal	Are unauthorized remote connections to the system monitored, including scanning for unauthorized mobile or wireless access points on a defined frequency and is appropriate action taken if an unauthorized connection is discovered?
320	Portable/Mobile/Wireless	Universal	Are wireless networking capabilities internally embedded within system components disabled prior to issue when not intended for use?
321	Portable/Mobile/Wireless	Universal	Are users NOT allowed to independently configure wireless networking capabilities?
322	Portable/Mobile/Wireless	Universal	Are users prohibited from establishing wireless networks?
323	Portable/Mobile/Wireless	Universal	Do you employ rigorous security measures for remote sessions with administrative privileges and are they audited?
324	Portable/Mobile/Wireless	Universal	Is peer-to-peer wireless networking capability disabled except for explicitly identified components in support of specific operational requirements?
325	System Protection	Universal	Does the system isolate (e.g., through partitions, domains, security zones, etc.) security functions (e.g., enforcing access and information flow control) functions from nonsecurity functions?
326	System Protection	Universal	Does the system isolate security functions from both nonsecurity functions and from other security functions?

327	System Protection	Universal	Does the system minimize the number of nonsecurity functions included within the isolation boundary containing security functions?
328	System Protection	Universal	Are the system security functions implemented as largely independent modules that avoid unnecessary interactions between modules?
329	System Protection	Universal	Are the system security functions implemented as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower defense in depth layers on the functionality or correctness of higher layers?
330	System Protection	Universal	Does the system limit the use of resources by priority?
331	System Protection	Universal	Are the external boundaries of the system defined?
332	System Protection	Universal	Are the operational system boundary, the strength required of the boundary, and the respective barriers to unauthorized access and control of system assets and components defined?
333	System Protection	Universal	Are externally accessible system components physically allocated to separate subnetworks (DMZ) with separate, physical network interfaces?
334	System Protection	Universal	Is external access into the organization's internal system networks prevented, except as appropriately mediated? (e.g., configuration files and settings, alarm points, passwords, etc.)
335	System Protection	Universal	Is an appropriate failure mode selected depending on the critical needs of system availability? (preventative maintenance)
336	System Protection	Universal	Does the system design and implementation protect the integrity of electronically communicated information?
337	System Protection	Universal	Is cryptographic hardware with remote key management capabilities used?
338	System Protection	Universal	Are public key certificates issued under an appropriate certificate policy or are they obtained under an appropriate certificate policy from an approved service provider?
339	System Protection	Universal	Does the use of public key certificates avoid degrading (i.e., latency) the operational performance of the system?
340	System Protection	Universal	Does the system fail to a known state for defined failures?
341	System Protection	Universal	Does the system preserve defined system state information in failure?
342	System Protection	Universal	Does the system employ processing components that have minimal functionality and data storage (e.g., diskless nodes, thin client technologies)?
343	System Protection	Universal	Does the system use secure data transmission media, such as fiber optic technology, to minimize data loss from eavesdropping and data tapping?
344	System Protection	Universal	Does the system protect the confidentiality of information at rest? (e.g., disk encryption)

345	System Protection	Universal	Are cryptographic mechanisms used to prevent unauthorized disclosure of information at rest unless otherwise protected by alternative physical measures?
346	System Protection	Universal	Are diverse technologies used in the implementation of the system? (e.g., using different vendors to avoid single vulnerability penetration)
347	System Protection	Universal	Are system components partitioned into separate physical networks as necessary?
348	System Protection	Universal	Does the system protect the integrity of information during the processes of data aggregation, packaging, and transformation in preparation for transmission?
349	System Protection	Universal	Does the system meet a defined level of trustworthiness?
350	System Protection	Universal	Are all critical hardware and software system components defined and documented?
351	System Protection	Universal	Has legacy equipment been updated with current or custom developed system components?
352	System Protection	Universal	Have system components been identified where there are no alternative sources or vendors?
353	System Protection	Universal	Is the system protected from harm by considering mean time to failure for a defined list of system components? (e.g., hot standby for real-time and/or application servers)
354	System Protection	Universal	Are substitute system components provided, and is there a mechanism to exchange active and standby roles of the components?
355	System Protection	Universal	Are system components taken out of service by transferring component responsibilities to a substitute component no later than a defined percentage of mean time to failure?
356	System Protection	Universal	Is a transfer between active and standby system components manually initiated at least once per a defined frequency?
357	System Protection	Universal	When a system component failure is detected, does the standby system component successfully and transparently assume its role within a defined time period and activate an alarm and/or automatically shut down the system?
358	System Protection	Universal	Is the use of personally owned information copied to the system restricted?
359	System Protection	Universal	Do the terms and conditions for personally owned information on the system state the types of applications that can be accessed from personally owned IT, either remotely or from within the system?
360	System Protection	Universal	Is the system configured to provide only essential capabilities and specifically prohibits and/or restricts the use of functions, ports, protocols, and/or services as defined in a "prohibited and/or restricted" list?

361	System Protection	Universal	Is the system periodically reviewed to identify and eliminate unnecessary functions, ports, protocols, and/or services?
362	System Protection	Universal	Are automated mechanisms used to prevent program execution in accordance with defined lists? (e.g., white listing)
363	System Protection	Universal	Are the use of configuration laptops and/or removable electronic media approved, and are authorized devices documented, secured, and available only to specified and approved entities when their use cannot be avoided?
364	System Protection	Universal	Is the enterprise architecture developed with consideration for security and the resulting risk?
365	System Protection	Universal	Do the terms and conditions for personally owned information on the system state the maximum security category of information that can be processed, stored, and transmitted?
366	System Protection	Universal	Do the terms and conditions for personally owned information on the system state how other users of the personally owned information will be prevented from accessing organization information?
367	System Protection	Universal	Do the terms and conditions for personally owned information on the system define the use of VPN and firewall technologies?
368	System Protection	Universal	Do the terms and conditions for personally owned information on the system state the use of and protection against the vulnerabilities of wireless technologies?
369	System Protection	Universal	Do the terms and conditions for personally owned information on the system require the maintenance of adequate physical security mechanisms?
370	System Protection	Universal	Do the terms and conditions for personally owned information on the system require the use of virus and spyware protection software?
371	System Protection	Universal	Do the terms and conditions for personally owned information on the system state how often the security capabilities of installed software are to be updated?
372	Software	Universal	Does the system include applications that are independent of the operating system?
373	Software	Universal	Are virtualization techniques used to present gateway components into systems environments as other types of components or components with differing configurations?
374	Software	Universal	Are virtualization techniques used to deploy a diversity of operating systems environments and applications?
375	Software	Universal	Is the diversity of operating systems and applications changed on a defined frequency?
376	Software	Universal	Is randomness used in the implementation of the virtualization?

377	Software	Universal	Does the system load and execute the operating system software from hardware-enforced, read-only media?
378	Software	Universal	Does the system load and execute authorized applications from hardware-enforced, read-only media?
379	Software	Universal	Are system components used that have no writable storage that is persistent across component restart or power on/off cycles?
380	Software	Universal	Is the integrity of the information on read-only media protected?
381	Software	Universal	Do software developers employ software quality and validation methods to minimize flawed or malformed software?
382	Software	Universal	Is a process prevented from executing without supervision for more than a defined time period?
383	Communication Protection	Universal	Is the system protected from information leakage (e.g., removable media, official documents, remote access, etc.)?
384	Communication Protection	Universal	Do the system components separate telemetry/data acquisition services from management port functionality?
385	Communication Protection	Universal	Does the system prevent unauthorized or unintended information transfer via shared system resources? (e.g., register, main memory, secondary storage)
386	Communication Protection	Universal	Does the system separate resources that are used to interface with systems operating at different security levels?
387	Communication Protection	Universal	Does the system monitor and manage communications at the system boundary and at key internal boundaries within the system?
388	Communication Protection	Universal	Are the number of access points to the system limited to allow for better monitoring of inbound and outbound network traffic?
389	Communication Protection	Universal	Is the external communication interface connections implemented with security measures appropriate to the required protection of the integrity and confidentiality of the information being transmitted?
390	Communication Protection	Universal	Does the system deny network traffic by default and allow network traffic by exception?
391	Communication Protection	Universal	Is the unauthorized release of information outside the system boundary or any unauthorized communication through the system boundary prevented when an operational failure occurs of the boundary protection mechanisms?
392	Communication Protection	Universal	Is the unauthorized release of information across managed interfaces prevented?

393	Communication Protection	Universal	Does the system check incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination?
394	Communication Protection	Universal	Does the system, at managed interfaces, deny network traffic and audit internal users posing a threat to external systems?
395	Communication Protection	Universal	Does the system prevent remote devices that have established connections (e.g., PLC, remote laptops) with the system from communicating outside that communications path with resources on uncontrolled/unauthorized networks?
396	Communication Protection	Universal	Does the system route traffic to the Internet through authenticated proxy servers within the managed interfaces of boundary protection devices?
397	Communication Protection	Universal	Do you encrypt communication over all untrusted communication channels?
398	Communication Protection	Universal	Have you evaluated the latency issues introduced by the use of cryptographic mechanisms to ensure that they do not impact operational performance?
399	Communication Protection	Universal	If the cryptographic mechanism fails, is your system protected against a denial of service event?
400	Communication Protection	Universal	Does the system design and implementation protect the confidentiality of communicated information where necessary?
401	Communication Protection	Universal	Are cryptographic mechanisms used to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures?
402	Communication Protection	Universal	Does the system establish a trusted communications path between the user and the system?
403	Communication Protection	Universal	Are cryptographic keys established and managed using automated mechanisms?
404	Communication Protection	Universal	Is the availability of information in the event of the loss of cryptographic keys by users maintained?
405	Communication Protection	Universal	Do communication cryptographic mechanisms comply with applicable regulatory requirements, policies, standards, and guidance?
406	Communication Protection	Universal	Are collaborative computing devices (e.g., video and audio conferencing) restricted on your control system network?
407	Communication Protection	Universal	Are collaborative computing devices disconnected and powered down when not in use?
408	Communication Protection	Universal	Does the system block both inbound and outbound traffic between instant messaging clients?

409	Communication Protection	Universal	Are collaborative computing devices disabled or removed from systems in secure work areas?
410	Communication Protection	Universal	Does the system reliably associate security labels and markings with information exchanged between the enterprise systems and the control system?
411	Communication Protection	Universal	Does the system validate the integrity of security parameters exchanged between systems?
412	Communication Protection	Universal	Is there usage restrictions and implementation guidance for VoIP technologies, which is based on the potential to cause damage to the system if used maliciously?
413	Communication Protection	Universal	Is the use of VoIP authorized, monitored, and controlled?
414	Communication Protection	Universal	Does the system provide mechanisms to protect the authenticity of device-to-device communications sessions?
415	Communication Protection	Universal	Are message authentication mechanisms implemented at the protocol level for both serial and routable protocols?
416	Communication Protection	Universal	Are the system devices that collectively provide name/address resolution services for an organization fault tolerant?
417	Communication Protection	Universal	Does the use of secure name/address resolution services avoid adverse impacts to the operational performance of the system?
418	Communication Protection	Universal	Does the DNS server that provides name/address resolution service provide additional artifacts (e.g., digital signatures, cryptographic keys, etc.) along with the authoritative DNS resource records it returns in response to resolution queries?
419	Communication Protection	Universal	Does the system enable verification of a chain of trust among parent and child domains?
420	Communication Protection	Universal	Does the local client perform DNS and data integrity verification from authoritative DNS servers?
421	Communication Protection	Universal	Does the authoritative DNS servers perform data origination and verification?
422	Communication Protection	Universal	Does the system monitor and detect covert communication channels (e.g., back doors)?
423	Communication Protection	Universal	Are a subset of the vendor-identified covert channel avenues tested to determine if they are exploitable?
424	Communication Protection	Universal	Does the system enforce assigned authorizations for controlling the flow of information within the system and between interconnected systems?

425	Communication Protection	Universal	Does the system enforce information flow control (e.g., firewalls, routers, gateways, etc.) based on specific data for source, and destination paths?
426	Communication Protection	Universal	Does the system enforce information flow control using domains as a basis for flow control decisions?
427	Communication Protection	Universal	Does the system enforce dynamic information flow control based on changing conditions or operational considerations?
428	Communication Protection	Universal	Does the system prevent encrypted data from bypassing content-checking mechanisms?
429	Communication Protection	Universal	Does the system enforce defined limitations on the embedding of data types within other data types to prevent propagation of malicious payloads?
430	Communication Protection	Universal	Does the system enforce information flow control on metadata?
431	Communication Protection	Universal	Does the system enforce defined one-way flows using hardware mechanisms (i.e., data diode)?
432	Communication Protection	Universal	Does the system enforce information flow control using defined security policy filters?
433	Communication Protection	Universal	Does the system enforce the use of human review for defined security policy filters when the system is not capable of making an information flow control decision?
434	Communication Protection	Universal	Does the system provide the capability for a privileged administrator to enable and disable organization-defined security policy filters?
435	Communication Protection	Universal	Does the system provide the capability for a privileged administrator to configure the organization-defined security policy filters to support different security policies?
436	Communication Protection	Universal	Is confidential information (e.g., business sensitive, personally identifiable information, etc.) restricted to authorized users?
437	Communication Protection	Universal	Are automated or manual mechanisms (e.g., roles and responsibilities as defined by Active Directory) used as required to assist authorizing users in making the correct information sharing/collaboration decisions?
438	Communication Protection	Universal	Is information sharing authorized and/or restricted between third-party partners?
439	Communication Protection	Universal	Are communications limited to only the devices that need to communicate?
440	Communication Protection	Universal	Are all other ports and routes locked down or disabled?
441	System Integrity	Universal	Are system flaws identified, reported, and corrected?

442	System Integrity	Universal	Are software updates tested related to flaw remediation for effectiveness and potential side effects before installation?
443	System Integrity	Universal	Is flaw remediation incorporated into the configuration management process as an emergency change?
444	System Integrity	Universal	Is the patch management process centrally managed, and are updates installed automatically?
445	System Integrity	Universal	Has the risk of employing automated flaw remediation been evaluated?
446	System Integrity	Universal	Are automated mechanisms (e.g., patching, service packs, etc.) used to periodically and on demand determine the state of system components with regard to flaw remediation?
447	System Integrity	Universal	Is the time between flaw identification and flaw remediation measured and compared with benchmarks?
448	System Integrity	Universal	Are automated patch management tools used to facilitate flaw remediation?
449	System Integrity	Universal	Does the use of automated flaw remediation processes NOT degrade the operational performance of the system?
450	System Integrity	Universal	Are system security alerts, advisories, and directives received from designated external organizations on an ongoing basis?
451	System Integrity	Universal	Are internal security alerts, advisories, and directives generated?
452	System Integrity	Universal	Are security alerts, advisories, and directives disseminated to a list of personnel?
453	System Integrity	Universal	Are security directives implemented in accordance with timeframes established by the directives, or is the issuing organization notified of the degree of noncompliance?
454	System Integrity	Universal	Are automated mechanisms used to make security alert and advisory information available throughout the organization?
455	System Integrity	Universal	Is the correct operation of security functions verified upon system startup and restart, upon command by user with appropriate privilege, periodically, and at defined time periods?
456	System Integrity	Universal	Does the system notify the system administrator when anomalies are discovered?
457	System Integrity	Universal	Are automated mechanisms used to provide notification of failed automated security tests?
458	System Integrity	Universal	Are automated mechanisms used to support management of distributed security functionality verification testing? (i.e., control log servers)
459	System Integrity	Universal	Does the system monitor and detect unauthorized changes to software and information?

460	System Integrity	Universal	Is the integrity of software and information reassessed by performing, on a defined frequency, integrity scans of the system, and are they used with extreme caution on designated high-availability systems?
461	System Integrity	Universal	Are automated tools used to provide notification to designated individuals on discovering discrepancies during integrity verification, and are they used with extreme caution on designated high-availability systems?
462	System Integrity	Universal	Are centrally managed integrity verification tools used, and are they used with extreme caution on designated high-availability systems?
463	System Integrity	Universal	Is tamper-evident packaging used during transportation from vendor to operational site, during operation, or both?
464	System Integrity	Universal	Does the system check the validity of information inputs? (e.g., boundary limits)
465	System Integrity	Universal	Does the system identify error conditions?
466	System Integrity	Universal	Does the system generate error messages that provide information necessary for corrective actions without revealing potentially harmful information that could be exploited by adversaries?
467	System Integrity	Universal	Does the system reveal error messages only to authorized personnel?
468	System Integrity	Universal	Does the system prohibit inclusion of sensitive information in error logs or associated administrative messages?
469	System Integrity	Universal	Is the output from the system handled and retained in accordance with applicable regulations, standards, and organizational policy as well as operational requirements?
470	Physical Security	Universal	Are lists of personnel with authorized access developed and maintained, and are appropriate authorization credentials issued?
471	Physical Security	Universal	Are the access list and authorization credentials reviewed and approved at least annually and those no longer requiring access removed?
472	Physical Security	Universal	Is physical access to the facility authorized based on position or role?
473	Physical Security	Universal	Are two forms of identification required to gain access to the facility?
474	Physical Security	Universal	Are physical access authorizations enforced for all physical access points to the facility?
475	Physical Security	Universal	Are individual access authorizations verified before granting access to the facility?
476	Physical Security	Universal	Is entry to the facility controlled by physical access devices and/or guards?
477	Physical Security	Universal	Are the areas officially designated as publicly accessible controlled in accordance with the organization's assessment of risk?
478	Physical Security	Universal	Are keys, combinations, and other physical access devices secured?

479	Physical Security	Universal	Are physical access devices inventoried on a periodic basis?
480	Physical Security	Universal	Are combinations and keys changed on a defined frequency, and when keys are lost, combinations compromised, or individuals are transferred or terminated?
481	Physical Security	Universal	Is physical access to distribution and communication lines controlled and verified?
482	Physical Security	Universal	Is physical access to output devices controlled?
483	Physical Security	Universal	Is physical access to the system controlled independently of the facility access controls?
484	Physical Security	Universal	Are security checks at physical boundaries performed for unauthorized removal of system components?
485	Physical Security	Universal	Is every physical access point to the facility guarded or alarmed and monitored 24 hours per day, 7 days per week?
486	Physical Security	Universal	Are lockable physical casings used to protect internal components of the system from unauthorized physical access?
487	Physical Security	Universal	Is physical access monitored to detect and respond to physical security incidents?
488	Physical Security	Universal	Are physical access logs reviewed on a defined frequency?
489	Physical Security	Universal	Are results of reviews and investigations coordinated with the organization's incident response capability?
490	Physical Security	Universal	Are real-time physical intrusion alarms and surveillance equipment monitored?
491	Physical Security	Universal	Are automated mechanisms used to recognize potential intrusions and initiate designated response actions?
492	Physical Security	Universal	Is physical access controlled by authenticating visitors before authorizing access?
493	Physical Security	Universal	Are visitors escorted and monitored as required in the security policies and procedures?
494	Physical Security	Universal	Are two forms of identification required for access?
495	Physical Security	Universal	Are visitor access records maintained, and are all physical access logs retained for as long as required by regulations or per approved policy?
496	Physical Security	Universal	Do visitor records include name and organization of the person visiting?
497	Physical Security	Universal	Do visitor records include the signature of the visitor?
498	Physical Security	Universal	Do visitor records include a form of identification?
499	Physical Security	Universal	Do visitor records include the date of access?
500	Physical Security	Universal	Do visitor records include the time of entry and departure?
501	Physical Security	Universal	Do visitor records include the purpose of the visit?
502	Physical Security	Universal	Do visitor records include the name and organization of person visited?

503	Physical Security	Universal	Are automated mechanisms employed to facilitate the maintenance and review of access records?
504	Physical Security	Universal	Is cryptographic hardware protected from physical tampering and uncontrolled electronic connections?
505	Physical Security	Universal	Are all external system and communication connections identified and protected from tampering or damage?
506	Physical Security	Universal	Are asset location technologies used to track and monitor the movements of personnel and vehicles to ensure they stay in authorized areas?
507	Physical Security	Universal	Are asset location technologies used to identify personnel needing assistance?
508	Physical Security	Universal	Are asset location technologies used to support emergency response?
509	Physical Security	Universal	Is hardware (cages, locks, cases, etc.) used to detect and deter unauthorized physical access to system devices?
510	Physical Security	Universal	Is the ability to respond to an emergency not hindered by using tamper-evident hardware?
511	Environmental Security	Universal	Is the emergency power shutoff protected from unauthorized activation?
512	Environmental Security	Universal	Is the emergency power-off capability protected from accidental and intentional/unauthorized activation?
513	Environmental Security	Universal	Is there a short-term uninterruptible power supply to be used for orderly system shutdown?
514	Environmental Security	Universal	Is there a long-term alternate power supply that is capable of maintaining minimally required operational capability?
515	Environmental Security	Universal	Is there a long-term alternate power supply that is self-contained and not reliant on external power generation?
516	Environmental Security	Universal	Are there automatic emergency lighting systems for emergency exits and evacuation routes?
517	Environmental Security	Universal	Are there fire suppression and detection devices/systems?
518	Environmental Security	Universal	Do fire detection devices/systems activate automatically and notify the organization and emergency responders in the event of a fire?
519	Environmental Security	Universal	Do fire suppression devices/systems provide automatic notification to the organization and emergency responders?
520	Environmental Security	Universal	Is there an automatic fire suppression capability in facilities that are not staffed continuously?

521	Environmental Security	Universal	Is the temperature and humidity regularly monitored to ensure they are maintained within acceptable levels?
522	Environmental Security	Universal	Is the system protected from water damage by having the master shutoff valves accessible, working properly, and known to key personnel?
523	Environmental Security	Universal	Are automated mechanisms used to close shutoff valves and provide notification in the event of a water leak?
524	Configuration Management	Universal	Is the delivery and removal of system components limited, authorized, and recorded?
525	Environmental Security	Universal	Are system assets located to minimize potential damage from physical and environmental hazards and to minimize unauthorized access?
526	Environmental Security	Universal	Are the risks associated with physical and environmental hazards considered when planning new system facilities or reviewing existing facilities, and are the risk mitigation strategies documented in the security plan?
527	Environmental Security	Universal	Is the system power equipment and power cabling protected from damage and destruction?
528	Environmental Security	Universal	Are redundant power equipment and parallel power cabling paths provided for the system?
529	Configuration Management	Universal	Is there an inventory of systems and critical components and is it maintained?
530	Plans	Universal	Are the personnel qualification levels reviewed and periodically updated for personnel to make changes, conditions for allowing changes, and the approvals required for changes?
531	Configuration Management	Universal	Has a current baseline configuration been developed, documented, and maintained for the system?
532	Configuration Management	Universal	Is the baseline configuration of the system reviewed and updated?
533	Configuration Management	Universal	Are automated mechanisms used to maintain an up-to-date, complete, accurate, and readily available baseline configuration?
534	Configuration Management	Universal	Is a baseline configuration for the development and test environments maintained and managed separately from the operational baseline?
535	Configuration Management	Universal	Is a deny-all, permit-by-exception authorization policy used for software allowed on the system?
536	Configuration Management	Universal	Are changes to the system authorized and documented?

537	Configuration Management	Universal	Are records of configuration-managed changes to the system reviewed and retained?
538	Configuration Management	Universal	Are configuration-managed changes to the system audited?
539	Configuration Management	Universal	Are automated mechanisms used to document proposed changes, notify appropriate approval authorities, highlight approvals that have not been received in a timely manner, inhibit change until necessary approvals are received, and document completed changes?
540	Configuration Management	Universal	Are configuration changes tested, validated, and documented before installing them on the operational system, and has testing been ensured to not interfere with system operations?
541	Configuration Management	Universal	Does the tester fully understand the corporate cyber and control system security policies and procedures and the specific health, safety, and environmental risks associated with a particular facility and/or process?
542	Configuration Management	Universal	Are individual access privileges, physical access, and logical access restrictions associated with configuration changes to the system defined, documented, and approved?
543	Configuration Management	Universal	Are individual access privileges, physical access, and logical access restrictions records associated with configuration changes to the system generated, retained, and periodically reviewed?
544	Configuration Management	Universal	Are automated mechanisms used to enforce change of access restrictions and support auditing of the enforcement actions?
545	Configuration Management	Universal	Does the system prevent the installation of device drivers that are not signed with an organizationally recognized and approved certificate?
546	Configuration Management	Universal	Is there physical security to restrict data devices, serial ports, network ports, USB, and secure digital memory card?
547	Configuration Management	Universal	Are mandatory configuration settings used for products employed within the system?
548	Configuration Management	Universal	Are the security settings configured to the most restrictive mode consistent with system operational requirements?
549	Configuration Management	Universal	Are the changed configuration settings documented?
550	Configuration Management	Universal	Are exceptions from the mandatory configuration settings identified, documented, and approved based on explicit operational requirements?

551	Configuration Management	Universal	Are the configuration settings for all components of the system enforced?
552	Configuration Management	Universal	Are changes to the configuration settings monitored and controlled in accordance with policies and procedures?
553	Configuration Management	Universal	Are automated mechanisms used to centrally manage, apply, and verify configuration settings?
554	Configuration Management	Universal	Are automated mechanisms used to respond to unauthorized changes to configuration settings?
555	Configuration Management	Universal	Is six wall bordering, equipment vaulting, two-man rules, and enhanced inventory control and authorization used?
556	Configuration Management	Universal	Are the duties and access between the system administrator and the cybersecurity officer separate such that neither can make the changes by themselves?
557	Configuration Management	Universal	Has an inventory of the components of the system been developed, documented and maintained that accurately reflects the current system?
558	Configuration Management	Universal	Has an inventory list of the components of the system been developed, documented, and maintained that is consistent with the system boundary?
559	Configuration Management	Universal	Has an inventory list of the components of the system been developed, documented, and maintained that is at the level of granularity deemed necessary for tracking and reporting?
560	Configuration Management	Universal	Has an inventory of the components of the system been developed, documented, and maintained that includes defined information deemed necessary to achieve effective property accountability?
561	Configuration Management	Universal	Is the inventory of system components and programming updated as an integral part of component installation, replacement, and system updates?
562	Configuration Management	Universal	Are automated mechanisms used to help maintain an up-to-date, complete, accurate, and readily available inventory of system components, configuration files and set points, alarm settings and other required operational settings?
563	Configuration Management	Universal	Are automated mechanisms used to detect the addition of unauthorized components/devices/component settings into the system?
564	Configuration Management	Universal	Is network access by unauthorized components/devices disabled, or are designated officials notified?
565	Configuration Management	Universal	Are the names of the individuals responsible for component included in property accountability information?

566	Configuration Management	Universal	Are all system assets and information documented, identified, and tracked?
567	Configuration Management	Universal	Do specialized critical digital assets have an internal registration, configuration and usage plan, and secure storage before, during, and after usage?
568	Configuration Management	Universal	Are critical digital assets (CDA) in security areas destroyed on removal from operations, or are they inspected and subject to an approved documented desanitization procedure on being removed from service (e.g., lifecycle plan)?
569	Configuration Management	Universal	Are all factory default authentication credentials changed on system components and applications upon installation?
570	Configuration Management	Universal	Does legacy equipment with known authentication deficiencies have compensatory access restrictions?
571	Plans	Universal	Is the responsibility for the configuration management process assigned to organizational personnel that are not directly involved in system development?
572	Configuration Management	Universal	Is there security authorization including two-man policies? (Requires the authorization of two people.)
573	Configuration Management	Universal	Are the legacy components identified, tested, and documented to verify that the compensatory measures are effective?
574	Incident Response	Universal	Are potential interruptions identified and classified as to "cause," "effects," and "likelihood"?
575	Incident Response	Universal	Is a root cause analysis initiated for the security events and any findings from the analysis submitted to the organizations corrective action program?
576	Incident Response	Universal	Is an incident handling capability implemented for security incidents that include preparation, detection and analysis, containment, eradication, and recovery?
577	Incident Response	Universal	Are incident handling activities coordinated with contingency planning activities?
578	Incident Response	Universal	Are lessons learned from ongoing incident handling activities incorporated into incident response procedures?
579	Incident Response	Universal	Are automated mechanisms used to administer and support the incident handling process and to assist in the reporting of security incidents?
580	Incident Response	Universal	Are system network security incidents tracked and documented on an ongoing basis?
581	Incident Response	Universal	Are automated mechanisms used to assist in the tracking of security incidents and in the collection and analysis of incident information? (e.g., network monitoring, physical access monitoring, etc.)
582	Incident Response	Universal	Are cyber and control system security incident information promptly reported to authorities?

583	Incident Response	Universal	Are automated mechanisms used to increase the availability of incident response-related information and support?
584	Incident Response	Universal	Is there a direct, cooperative relationship between the incident response capability and external providers of information system protection capability, and are the incident response team members identified to the external providers? (e.g., third party alarm service)
585	Incident Response	Universal	Are processes and mechanisms included in the planning to ensure that corrective actions identified as the result of a cybersecurity incident are fully implemented?
586	Incident Response	Universal	Does the incident response capability incorporate detection of unauthorized, security-relevant configuration changes to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes?
587	Incident Response	Universal	Is an incident response support resource provided that offers advice and assistance?
588	Monitoring & Malware	Universal	Does the system protect against or limit the effects of denial-of-service attacks based on a defined list of types of denial-of-service attacks?
589	Monitoring & Malware	Universal	Does the system restrict the ability of users to launch denial-of-service attacks against other systems or networks?
590	Monitoring & Malware	Universal	Does the system manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks?
591	Monitoring & Malware	Universal	Are malicious code protection mechanisms used at system entry and exit points and at workstations, servers, or mobile computing devices?
592	Monitoring & Malware	Universal	Are malicious code protection mechanisms updated whenever new releases are available in accordance with configuration management policy and procedures?
593	Monitoring & Malware	Universal	Are malicious code protection mechanisms configured to perform periodic scans of the system on a defined frequency and real-time scans of files from external sources as the files are downloaded, opened, or executed, and disinfect and quarantine infected files?
594	Monitoring & Malware	Universal	Are malicious code protection software products from multiple vendors used?
595	Monitoring & Malware	Universal	Are the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system addressed?
596	Monitoring & Malware	Universal	Are malicious code protection mechanisms centrally managed?
597	Monitoring & Malware	Universal	Does the system automatically update malicious code protection mechanisms?

598	Monitoring & Malware	Universal	Does the system prevent users from circumventing host-based malicious code protection capabilities?
599	Monitoring & Malware	Universal	Does the system update malicious code protection mechanisms only when directed by a privileged user?
600	Monitoring & Malware	Universal	Are users prohibited from introducing removable media into the system?
601	Monitoring & Malware	Universal	Does the system implement malicious code protection mechanisms to identify data containing malicious code and respond accordingly when the system encounters data not explicitly allowed by the security policy?
602	Monitoring & Malware	Universal	Does the use of mechanisms to centrally manage malicious code protection avoid degradation of the operational performance of the system?
603	Monitoring & Malware	Universal	Are periodic security vulnerability assessments conducted according to the risk management plan?
604	Monitoring & Malware	Universal	Is the system updated to address any identified vulnerabilities in accordance with the system maintenance policy?
605	Monitoring & Malware	Universal	Are events on the system monitored?
606	Monitoring & Malware	Universal	Are system attacks detected? (Attacks can be detected via log monitoring, IDS system monitoring, Signature/indicators)
607	Monitoring & Malware	Universal	Is unauthorized use of the system identified? (e.g., log monitoring)
608	Monitoring & Malware	Universal	Are monitoring devices deployed strategically to collect essential information within the system to track specific types of transactions of interest?
609	Monitoring & Malware	Universal	Is the level of system monitoring activity heightened whenever an indication of increased risk exists?
610	Monitoring & Malware	Universal	Is legal counsel consulted with regard to system monitoring activities?
611	Monitoring & Malware	Universal	Are individual intrusion detection tools interconnected into a systemwide intrusion detection system?
612	Monitoring & Malware	Universal	Are automated tools used to support near real-time analysis of events?
613	Monitoring & Malware	Universal	Are automated tools used to integrate intrusion detection tools into access control and flow control mechanisms in support of attack isolation and elimination?

614	Monitoring & Malware	Universal	Does the system monitor inbound and outbound communications for unusual or unauthorized activities or conditions?
615	Monitoring & Malware	Universal	Does the system provide a real-time alert when indications of compromise or potential compromise occur?
616	Monitoring & Malware	Universal	Does the system prevent users from circumventing host-based intrusion detection and prevention capabilities?
617	Monitoring & Malware	Universal	Does the system notify a list of incident response personnel of suspicious events and take the least disruptive actions to terminate suspicious events?
618	Monitoring & Malware	Universal	Is information obtained from intrusion monitoring tools protected from unauthorized access, modification, and deletion?
619	Monitoring & Malware	Universal	Are intrusion monitoring tools tested on a defined time-period?
620	Monitoring & Malware	Universal	Is encrypted traffic visible to system monitoring tools?
621	Monitoring & Malware	Universal	Does the use of monitoring tools and techniques avoid adversely impacting the operational performance of the system?
622	Monitoring & Malware	Universal	Are spam protection mechanisms used at system entry points and at workstations, servers, or mobile computing devices?
623	Monitoring & Malware	Universal	Are spam protection mechanisms updated when new releases are available in accordance with configuration management policy and procedures?
624	Monitoring & Malware	Universal	Is spam protection software products from multiple vendors used?
625	Monitoring & Malware	Universal	Are spam protection mechanisms centrally managed and has the risk of employing mechanisms to centrally manage spam protection on a system been considered?
626	Monitoring & Malware	Universal	Does centrally managed spam protection avoid degrade the operational performance of the system?
627	Monitoring & Malware	Universal	Have you considered the risks of automatically updating spam protection mechanisms on high-availability systems?
628	Monitoring & Malware	Universal	Does the system include components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, analyzing, and tracking such attacks? (e.g., honeypots)
629	Monitoring & Malware	Universal	Does the system include components that proactively seek to identify Web-based malicious code?

630	Monitoring & Malware	Universal	Are vulnerability scans performed for in the system on a defined frequency and randomly in accordance with company policy?
631	Monitoring & Malware	Universal	Are vulnerability scanning tools and techniques used that promote interoperability among tools and automate parts of the vulnerability management process by using standards for: (a) enumerating platforms, software flaws, and improper configurations; (b) formatting and making transparent, checklists, and test procedures; and (c) measuring vulnerability impact?
632	Monitoring & Malware	Universal	Is information obtained from the vulnerability scanning process shared with designated personnel throughout the organization?
633	Monitoring & Malware	Universal	Are vulnerability scanning tools used that include the capability to readily update the list of system vulnerabilities scanned?
634	Monitoring & Malware	Universal	Is the list of system vulnerabilities scanned updated on a defined frequency or when new vulnerabilities are identified and reported?
635	Monitoring & Malware	Universal	Are there vulnerability scanning procedures that can demonstrate the breadth and depth of coverage?
636	Monitoring & Malware	Universal	Does the organization attempt to discern what information about the system is discoverable by adversaries?
637	Monitoring & Malware	Universal	Is security testing performed to determine the level of difficulty in circumventing the security controls of the system?
638	Monitoring & Malware	Universal	Are privileged access vulnerability scans performed on selected system components?
639	Monitoring & Malware	Universal	Are automated mechanisms used to compare the results of vulnerability scans over time to determine trends in system vulnerabilities?
640	Monitoring & Malware	Universal	Are automated mechanisms used on a defined frequency to detect the presence of unauthorized software on organizational systems and notify designated officials?
641	Continuity	Universal	Are backups of critical system software, applications, and data created and secured?
642	Continuity	Universal	Is normal operation of the system resumed in accordance with its policies and procedures after a security event?
643	Continuity	Universal	Is an alternate storage site identified and are agreements in place to permit the storage of system configuration information?
644	Continuity	Universal	Are potential accessibility problems at the alternative storage site identified in the event of an areawide disruption or disaster and are explicit mitigation actions outlined?

645	Continuity	Universal	Is an alternate storage site identified that is geographically separated from the primary storage site?
646	Continuity	Universal	Is the alternate storage site configured to facilitate timely and effective recovery operations?
647	Continuity	Universal	Are alternate command/control methods identified, and are agreements in place to permit the resumption of operations within a defined time period when the primary system capabilities are unavailable?
648	Continuity	Universal	Do primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the availability requirements?
649	Continuity	Universal	Do alternate telecommunications services avoid sharing a single point of failure with primary telecommunications services (e.g., radio and lease lines)?
650	Continuity	Universal	Are alternate telecommunications service providers sufficiently separated from primary service providers?
651	Continuity	Universal	Do primary and alternate telecommunications service providers have adequate contingency plans?
652	Continuity	Universal	Are necessary communications for the alternate control center identified, and are agreements in place to permit the resumption of system operations for critical functions within a defined time period when the primary control center is unavailable?
653	Continuity	Universal	Is an alternate control center identified that is geographically separated from the primary control center?
654	Continuity	Universal	Are potential accessibility problems to the alternate control center identified in the event of an area-wide disruption or disaster and are explicit mitigation actions outlined?
655	Continuity	Universal	Are alternate control center agreements in place that contain priority-of-service provisions in accordance with the availability requirements?
656	Continuity	Universal	Is the alternate control center fully configured to be used as the operational site supporting a minimum required operational capability?
657	Continuity	Universal	Does the alternate processing site provide information security measures equivalent to that of the primary site?
658	Continuity	Universal	Are backups of user-level information contained in the system performed on a defined frequency? (user account)
659	Continuity	Universal	Are backups of system-level information contained in the system performed on a defined frequency?

660	Continuity	Universal	Is the confidentiality and integrity of backup information protected at the storage location?
661	Continuity	Universal	Is backup information periodically tested to verify media reliability and information integrity?
662	Continuity	Universal	Is backup information selectively used in the restoration of system functions as part of contingency plan testing?
663	Continuity	Universal	Are backup copies of the operating system and other critical system software stored in a separate facility or in a fire-rated container that is not collocated with the operational software?
664	Continuity	Universal	Is there a capability to recover and reconstitute the system to a known secure state after a disruption, compromise, or failure?
665	Continuity	Universal	Is there transaction recovery for systems that are transaction-based?
666	Continuity	Universal	Is there a capability to re-image system components within defined restoration time periods from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components?
667	Continuity	Universal	Is the system able to execute an appropriate fail-safe procedure upon the loss of communications with the system or the loss of the system itself?
668	Continuity	Universal	Does the system preserve the system state information in failure?
669	Info Protection	Universal	Do only authorized users have access to information in printed form or on digital media?
670	Info Protection	Universal	Are automated mechanisms (e.g., card or keypad entry) used to ensure and audit authorized access to media storage areas?
671	Info Protection	Universal	Is all removable information storage media and the system output reviewed and classified to determine distribution limitations?
673	Info Protection	Universal	Is a defined list of media types or hardware components exempted from marking as long as the exempted items remain within the protected environment?
674	Info Protection	Universal	Does the system mark output on external media to identify any of the set of special dissemination, handling, or distribution instructions that apply to system output using human readable, standard naming conventions?
675	Info Protection	Universal	Is the system media securely stored within protected areas?
676	Info Protection	Universal	Does the sensitivity of the material determine how the media are stored?
677	Info Protection	Universal	Are defined types of digital and nondigital media protected during transport outside controlled areas?

678	Info Protection	Universal	Is accountability for system media maintained during transport outside controlled areas?
679	Info Protection	Universal	Are the activities associated with transport of media restricted to authorized personnel?
680	Info Protection	Universal	Are activities associated with the transport of system media documented using a defined system of records?
681	Info Protection	Universal	Is a custodian identified throughout the transport of system media?
682	Info Protection	Universal	Is system digital and nondigital media sanitized before disposal or release for reuse?
683	Info Protection	Universal	Are media sanitization and disposal actions tracked, documented, and verified?
684	Info Protection	Universal	Are sanitization equipment and procedures periodically tested to verify correct performance?
685	Info Protection	Universal	Are the individuals designated who are authorized to post information onto an organizational system that is publicly accessible?
686	Info Protection	Universal	Are authorized individuals trained to ensure that publicly accessible information does not contain nonpublic information?
687	Info Protection	Universal	Is the proposed content of publicly accessible information reviewed prior to posting?
688	Info Protection	Universal	Is the content on the publicly accessible organizational information system reviewed on a routine interval?
689	Info Protection	Universal	Is nonpublic information removed from publicly accessible information systems if discovered?
690	Info Protection	Universal	Is all information classified to indicate the protection required in accordance with its sensitivity and consequence?
691	Access Control	Universal	Are formal contractual and confidentiality agreements established for the exchange of information and software between the organization and external parties?
692	Info Protection	Universal	Is information that requires special control or handling periodically reviewed to determine whether such special handling is still required?
693	Info Protection	Universal	Is removable system media and system output marked indicating the distribution limitations, handling caveats, and applicable security markings?
694	Info Protection	Universal	Is there a list of media types or hardware components that is exempt from marking as long as the exempted items remain within the organization-defined protected environment?
695	Information and Document Management	Universal	Does the system automatically label information in storage, in process, and in transmission in accordance with access control requirements?

696	Information and Document Management	Universal	Is information labeled in storage, in process, and in transmission in accordance with special dissemination, handling, or distribution instructions?
697	Information and Document Management	Universal	Does the system automatically label information in storage, in process, and in transmission as required by the system security policy?
698	Information and Document Management	Universal	Does the system dynamically reconfigure security attributes in accordance with an identified security policy as information is created and combined?
699	Information and Document Management	Universal	Does the system allow authorized entities to change security attributes?
700	Information and Document Management	Universal	Does the system maintain the binding of security attributes to information with sufficient assurance that the information attribute association can be used as the basis for automated policy actions?
701	Information and Document Management	Universal	Does the system allow authorized users to associate security attributes with information?
702	Information and Document Management	Universal	Does the system display security attributes in human-readable form on each object-output from the system-to-system output devices to identify special dissemination, handling, or distribution instructions?
703	Information and Document Management	Universal	Is administrator and user guidance for the system obtained, protected and provided that includes configuring, installing, and operating the system and use of the system's security features?
704	Information and Document Management	Universal	Is vendor/contractor information obtained, protected, and made available to authorized personnel that describes the functional properties of the security controls within the system?
705	Information and Document Management	Universal	Is vendor/contractor information obtained, protected, and made available to authorized personnel that describes the design and implementation details of the security controls within the system?
706	Information and Document Management	Universal	Is vendor/contractor information obtained, protected, and made available to authorized personnel that describes the security-relevant external interfaces to the system?

707	Information and Document Management	Universal	Are software and associated documentation used in accordance with contract agreements and copyright laws?
708	Information and Document Management	Universal	Are tracking systems used to control copying and distribution of software and associated documentation protected by quantity licenses?
709	Information and Document Management	Universal	Is the use of accessible peer-to-peer file sharing technology controlled and documented to ensure that it is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work?
710	System and Services Acquisition	Universal	Are security functional requirements and specifications included in system acquisition contracts based on an assessment of risk?
711	System and Services Acquisition	Universal	Are security-related documentation requirements included in system acquisition contracts based on an assessment of risk?
712	System and Services Acquisition	Universal	Are developmental and evaluation-related assurance requirements (acceptance testing, compliance documentation) included in system acquisition contracts based on an assessment of risk?
713	System and Services Acquisition	Universal	Do acquisition documents require that vendors/contractors provide information describing the functional properties of the security controls employed within the system?
714	System and Services Acquisition	Universal	Do acquisition documents require that vendors/contractors provide information describing the design and implementation details of the security controls employed within the system?
715	System and Services Acquisition	Universal	Is the acquisition of commercial technology products with security capabilities limited to products that have been evaluated and validated?
716	System and Services Acquisition	Universal	Are system security engineering principles applied in the specification, design, development, and implementation of the system?
717	System and Services Acquisition	Universal	Are software development standards and practices for trustworthy software used throughout the development life cycle?
718	System and Services Acquisition	Universal	Are software practices used to reduce buffer overflows and unsafe string management for languages that have unsafe operations?
719	System and Services Acquisition	Universal	As part of trustworthy software development are commercially available tools employed, including a robust set of data validation and software quality assurance?

720	System and Services Acquisition	Universal	Are providers of external system services required to employ security controls in accordance with applicable, policies, regulations, standards, guidance, and established service level agreements?
721	System and Services Acquisition	Universal	Are government oversight and user roles and responsibilities defined with regard to external system services?
722	System and Services Acquisition	Universal	Is security control compliance by external service providers monitored?
723	System and Services Acquisition	Universal	Are system developers/integrators required to implement and document a configuration management process that manages and controls changes to the system during design, development, implementation, and operation?
724	System and Services Acquisition	Universal	Are system developers/integrators required to implement and document a configuration management process that tracks security flaws?
725	System and Services Acquisition	Universal	Are system developers/integrators required to implement and document a configuration management process that includes organizational approval of changes?
726	System and Services Acquisition	Universal	Are system developers/integrators required to provide an integrity check of software?
727	System and Services Acquisition	Universal	Is an alternative configuration management process provided in the absence of a dedicated developer/integrator configuration management team?
728	System and Services Acquisition	Universal	Does the system developer have a security test and evaluation plan?
729	System and Services Acquisition	Universal	Does the system developer have a verifiable error remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process?
730	System and Services Acquisition	Universal	Does the system developer/integrator document the result of the security testing/evaluation and error remediation processes?
731	System and Services Acquisition	Universal	Does the system developer/integrator employ code analysis tools to examine software for common flaws and document the results of the analysis?
732	System and Services Acquisition	Universal	Does the system developer/integrator perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations?
733	System and Services Acquisition	Universal	Is the test and evaluation plan under independent verification and validation?
734	System and Services Acquisition	Universal	Are supply chain vulnerabilities protected from threats initiated against organizations, people, information, and resources that provide products or services to the organization?

735	System and Services Acquisition	Universal	Are all anticipated system components and spares purchased in the initial acquisition?
736	System and Services Acquisition	Universal	Are trusted intermediaries used for purchasing contract services, acquisitions, or logistical activities during the system life cycle?
737	System and Services Acquisition	Universal	Is a due diligence review conducted of suppliers prior to entering into contractual agreements to acquire system hardware, software, firmware, or services?
738	System and Services Acquisition	Universal	Is trusted shipping and warehousing used for systems, components, and technology products?
739	System and Services Acquisition	Universal	Are a diverse set of suppliers used for systems, components, technology products, and system services?
740	System and Services Acquisition	Universal	Are standard configurations used for systems, components, and technology products?
741	System and Services Acquisition	Universal	Is the time between purchase decisions and delivery minimized for systems, components, and technology products?
742	System and Services Acquisition	Universal	Are independent analysis and penetration testing performed on delivered systems, components, and technology products?
743	Maintenance	Universal	Are security requirements for the system reviewed and followed before undertaking any unplanned maintenance activities?
744	Maintenance	Universal	Does unplanned maintenance documentation include: (a) date and time, (b) name of the those performing the maintenance, (c) escorts name, (d) description of the maintenance performed, and (e) list of equipment removed or replaced?
745	Maintenance	Universal	Is the decision not to perform emergency repairs maintenance after the identification of a security vulnerability documented and justified?
746	Maintenance	Universal	Are repairs and maintenance scheduled, performed, and documented, and are records reviewed in accordance with manufacturer or vendor specifications and/or organizational requirements?
747	Maintenance	Universal	Is the removal of the system or system components from organizational facilities for offsite maintenance or repairs approved?
748	Maintenance	Universal	Is the equipment sanitized to remove all information from associated media prior to removal from organizational facilities for offsite maintenance or repairs?
749	Maintenance	Universal	Are all potentially impacted security controls checked to verify that the controls are still functioning properly following maintenance or repair actions?

750	Maintenance	Universal	Are maintenance records for the system maintained and do they include: (a) date and time, (b) name of those performing the maintenance, (c) escorts name, (d) description of the maintenance performed, and (e) list of equipment removed or replaced?
751	Maintenance	Universal	Are automated mechanisms used to schedule and document maintenance and repairs?
752	Maintenance	Universal	Is the use of system maintenance tools approved and monitored?
753	Maintenance	Universal	Are all maintenance software tools carried into a facility inspected for obvious improper modifications?
754	Maintenance	Universal	Are all media containing diagnostic and test programs checked for malicious code before the media are used in the system?
755	Maintenance	Universal	Is the unauthorized removal of maintenance equipment prevented by one of the following: (a) verifying that no organizational information is contained on the equipment, (b) sanitizing or destroying the equipment, (c) retaining the equipment within the facility, or (d) obtaining an exemption from a designated organization official explicitly authorizing removal of the equipment?
756	Maintenance	Universal	Are automated mechanisms used to restrict the use of maintenance tools to authorized personnel only?
757	Maintenance	Universal	Are maintenance software tools used with care on system networks to ensure that system operations will not be degraded by their use?
758	Maintenance	Universal	Are only authorized and qualified organization or vendor personnel allowed to perform maintenance on the system?
759	Maintenance	Universal	Are remotely executed maintenance and diagnostic activities authorized, monitored, and controlled?
760	Maintenance	Universal	Are remote maintenance and diagnostic tools used only as consistent with policy and documented in the security plan for the system?
761	Maintenance	Universal	Are records for remote maintenance and diagnostic activities maintained?
762	Maintenance	Universal	Are all sessions and remote connections terminated when remote maintenance is completed?
763	Maintenance	Universal	Are passwords changed following each remote maintenance session if password-based authentication is used to accomplish remote maintenance?
764	Maintenance	Universal	Are remote maintenance and diagnostic sessions audited and do designated organizational personnel review the maintenance records of the remote sessions?
765	Maintenance	Universal	Is the installation and use of remote maintenance and diagnostic links documented?

766	Maintenance	Universal	Are remote maintenance or diagnostic services required to be performed from a system that implements a level of security at least as high as that implemented on the system being serviced, or is the component to be serviced sanitized and removed from the system prior to remote maintenance or diagnostic services?
767	Maintenance	Universal	Is the authorized firmware code checked or reinstalled as specified by the configuration management plan, and are all authorized embedded configuration settings reset after component servicing and return of the component to the facility but before reconnecting the component to the system?
768	Maintenance	Universal	Are the remote maintenance sessions protected by a strong authenticator tightly bound to the user?
769	Maintenance	Universal	Do maintenance personnel notify the system administrator when remote maintenance is planned, and does a designated official with specific security/system knowledge approve the remote maintenance?
770	Maintenance	Universal	Are cryptographic mechanisms used to protect the integrity and confidentiality of remote maintenance and diagnostic communications?
771	Maintenance	Universal	Is remote disconnect verification used at the termination of remote maintenance and diagnostic sessions?
772	Maintenance	Universal	Is there maintenance support and spare parts for security-critical system components within the period of failure?
773	Audit and Accountability	Universal	Is there a frequency of auditing for each identified auditable event?
774	Audit and Accountability	Universal	Is the security audit function coordinated with other organizational entities requiring audit-related information?
775	Audit and Accountability	Universal	Are auditable events adequate to support after-the-fact investigations of security incidents?
776	Audit and Accountability	Universal	Are the events to be audited adjusted within the system based on current threat information and ongoing assessments of risk?
777	Audit and Accountability	Universal	Is the list of defined auditable events reviewed and updated on a defined frequency?
778	Audit and Accountability	Universal	Is execution of privileged functions (account creations, modifications, and object permission changes) included in the list of events to be audited by the system?
779	Audit and Accountability	Universal	Are audit records produced that contain sufficient information to establish what events occurred, when the events occurred, where the events occurred, the sources of the events, and the outcomes of the events?

780	Audit and Accountability	Universal	Is there the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject?
781	Audit and Accountability	Universal	Is there the capability to centrally manage the content of audit records generated by individual hardware and/or software components throughout the system?
782	Audit and Accountability	Universal	Is there sufficient audit record storage capacity allocated and is auditing configured to reduce the likelihood of such capacity being exceeded?
783	Audit and Accountability	Universal	Does the system alert designated organizational officials in the event of an audit processing failure?
784	Audit and Accountability	Universal	Does the system take the following actions: (e.g., shutdown system, overwrite oldest audit records, stop generating audit records).
785	Audit and Accountability	Universal	Does the system provide a warning when allocated audit record storage volume reaches a defined percentage of maximum storage capacity?
786	Audit and Accountability	Universal	Is there a real-time alert when any defined event occurs?
787	Audit and Accountability	Universal	Does the system enforce configurable traffic volume thresholds representing auditing capacity for network traffic, and does the system either reject or delay network traffic above those thresholds?
788	Audit and Accountability	Universal	Are system audit records reviewed and analyzed on a defined frequency, and are findings reported to designated officials?
789	Audit and Accountability	Universal	Is the level of audit review, analysis, and reporting within the system adjusted when a change in risk exists?
790	Audit and Accountability	Universal	Are automated mechanisms used to integrate audit review, analysis, and reporting into processes for investigation and response to suspicious activities?
791	Audit and Accountability	Universal	Are audit records analyzed and correlated across different repositories?
792	Audit and Accountability	Universal	Are automated mechanisms used to centralize audit review and analysis of audit records from multiple components within the system?
793	Audit and Accountability	Universal	Is the analysis of audit records integrated with analysis of performance and network monitoring information?
794	Audit and Accountability	Universal	Does the system provide an audit reduction and report generation capability?
795	Audit and Accountability	Universal	Is there the capability to automatically process audit records for events of interest based on selectable event criteria?

796	Audit and Accountability	Universal	Does audit record processing avoid degrading the operational performance of the system?
797	Audit and Accountability	Universal	Does the system use internal system clocks to generate time stamps for audit records?
798	Audit and Accountability	Universal	Does the system synchronize internal system clocks on a defined frequency?
799	Audit and Accountability	Universal	Does the system protect audit information and audit tools from unauthorized access, modification, and deletion?
800	Audit and Accountability	Universal	Does the system produce audit records on hardware-enforced, write-once media (e.g., CD, DVD, etc.)?
801	Audit and Accountability	Universal	Are audit logs retained for a defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements?
802	Audit and Accountability	Universal	Are audits conducted at planned intervals to determine whether the security objectives, measures, processes, and procedures conform to the requirements and relevant legislation or regulations?
803	Audit and Accountability	Universal	Are audits conducted at planned intervals to determine whether the security objectives, measures, processes, and procedures conform to the identified information security requirements?
804	Audit and Accountability	Universal	Are audits conducted at planned intervals to determine whether the security objectives, measures, processes, and procedures are effectively implemented and maintained?
805	Audit and Accountability	Universal	Are audits conducted at planned intervals to determine whether the security objectives, measures, processes, and procedures perform as expected?
806	Audit and Accountability	Universal	Are audits conducted at planned intervals to determine whether the security objectives, measures, processes, and procedures identify inappropriate activities?
807	Audit and Accountability	Universal	Does the audit program specify the auditor qualifications?
808	Audit and Accountability	Universal	Are the auditor and system administration functions assigned to separate personnel?
809	Audit and Accountability	Universal	Do the audit program specify strict rules and careful use of audit tools when auditing system functions, especially with legacy systems?
810	Audit and Accountability	Universal	Is extra care taken to ensure that automated scanning tools used on the business networks do not scan the ICS network by mistake?

811	Audit and Accountability	Universal	Is compliance to the security policy demonstrated through audits in accordance with the audit program?
812	Audit and Accountability	Universal	Does the system provide audit record generation capability for the auditable events?
813	Audit and Accountability	Universal	Does the system provide audit record generation capability of the defined system components?
814	Audit and Accountability	Universal	Are authorized users allowed to select which auditable events are to be audited by specific components of the system?
815	Audit and Accountability	Universal	Are audit records generated for the selected list of auditable events?
816	Audit and Accountability	Universal	Does the system provide the capability to compile audit records from multiple components within the system into a systemwide audit trail that is time-correlated to within a defined level of tolerance (e.g., time sync on audit logs, centralized log server, etc.)?
817	Audit and Accountability	Universal	Is open source information monitored for evidence of unauthorized release or disclosure of organizational information?
818	Audit and Accountability	Universal	Does the system provide the capability to capture, record, and log all content related to a user session where it is required?
819	Audit and Accountability	Universal	Does the system provide the capability to remotely view all content related to an established user session in real time where legally required?
820	Audit and Accountability	Universal	Are audits of system changes done at a defined frequency, and when indications warrant to determine whether unauthorized changes have occurred?
821	Audit and Accountability	Universal	Is the level of audit review, analysis, and reporting adjusted when there is a change in risk?
822	Audit and Accountability	Universal	Are automated mechanisms used to integrate audit review, analysis, and reporting for investigation and response to suspicious activities?
823	Audit and Accountability	Universal	Are automated mechanisms used to centralize audit review and analysis records from multiple components within the system?
824	Audit and Accountability	Universal	Is analysis of audit records integrated with analysis of performance and network monitoring information to identify inappropriate or unusual activity?