Cyber IST Questions

January 2014

Version 1.1.10 (01-09-14)

Homeland Security

This page is intentionally left blank

OMB Control Number: 1670-NEW
Expiration Date: XX/XX/XXXX

Privacy Act Statement:
Authority: 44 U.S.C. § 3101 and 44 U.S.C. § 3534 authorize the collection of this information.
Purpose: DHS will use this information to create and manage your user account and grant access to the Infrastructure Protection (IP) Gateway.
Routine Use: This information may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974. This includes using the information, as necessary and authorized by the routine uses published in DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS) November 27, 2012, 77 Fed. Reg. 70,792.
Disclosure: Furnishing this information is voluntary; however failure to provide the information requested may delay or prevent DHS from processing your access request.

Paperwork Reduction Act: The public reporting burden to complete this information collection is estimated at 7.5 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and the completing and reviewing the collected information. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number and expiration date. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to DHS/NPPD/IICD, Kimberly Sass, Kimberly.sass@hq.dhs.gov ATTN: PRA [OMB Control Number 1670-New].

This page is intentionally left blank

Contents

Document History

Required Version	Description of Change	Author	Date
1.0	Initial draft.	Nate Evans	29 April 13
1.1	Clean version produced from initial comments.	Nate Evans	7 June 13
1.1.1	Edits from various conversations and collaborations between Evans and Willke.	Nate Evans	30 June 13
1.1.2	Edits to update language. General Section and Document History added.	Nate Evans	1 July 13
1.1.3	Edits from conversation with Willke on July 1, 2013. Staffing Section added. General Section modified.	Nate Evans	2 July 13
1.1.4	Edits to map to NIST framework/ standards and reduce question set.	Nate Evans and Rebecca Haffenden	2 August 13
1.1.5	Updated to reflect organizational changes and to change “system” to “service.”	Nate Evans	14 August 13
1.1.6	Updated on the basis of testing.	Nate Evans and Bradford Willke	26 August 13
1.1.7	Updated based on SLTT Feedback	Nate Evans and Bradford Willke	26 September 13
1.1.8	Updated based on Lab Cyber Elicitation	Amanda Theel, Nate Evans, Bill Buehring, and Angeli Tompkins	18 November 13
1.1.9	Updated based on SLTT Cyber Elicitation	Amanda Theel, Nate Evans, Bill Buehring, and Angeli Tompkins	22 November 13
1.1.10	Edits and updates of ‘helps’	Amanda Theel	9 January 14

1.0 Background Information

1.1 Primary Cyber or Cyber Security Point of Contact

Include a single Point Of Contact (POC.) Typically this is the primary POC for the company and the 24 hour contact and is the person that will receive the dashboard. On occasion, the Cyber POC will not be the owner / operator.

1.2 Technical Operator Contact that Should Receive Primary Access to the Cyber Survey Dashboard

Please identify the individual that will be the primary user of the dashboard; if applicable, please select the individual that has signed the E&C. This user will be able to create additional users for the site.

1.2 Other Organizations and Visit Participants / Emergency Communications

List all persons contacted during the assessment or that was provided by the owner. If the person participated in the assessment select the box indicating participated in survey.

List all protocols/services that are contacted for emergency communications in an event of an incident or disaster for this site.

Primary Cyber or Cyber Security Point of Contact (POC)	
First Name	_____
Last Name	_____
Title	_____
Company/Agency	_____
Phone	Office: _____ Cell: _____
Email	_____
Report to	_____

☐ Dashboard recipient
☐ Participated in site visit

Technology Operator Contact (may be different from the Primary Cyber or Cyber Security Point of Contact)	
Same as Primary POC ☐	
First Name	_____
Last Name	_____
Title	_____
Company/Agency	_____
Phone	Office: _____ Cell: _____
Email	_____
Report to	_____

☐ Dashboard recipient
☐ Participated in site visit

Other Organization Contact or Visit Participant (replicate as needed)	
First Name	_____
Last Name	_____
Company/Agency	_____
Title/Position	_____
Phone	Office: _____ Cell: _____
Email	_____

☐ Participated in site visit

Emergency Communications

Protocol for Emergency Communications	_____

2.0 General Information

2.1 What is a Critical Cyber Service?

A basic principle to remember throughout the survey is, "What is a 'Critical Cyber Service." A cyber service is any combination of equipment and devices (hardware); applications and platforms (software), communications, and data that is integrated to provide specific cyber services. A critical cyber service (CCS) is a service that the loss thereof would result in physical destruction, safety, and health effects (e.g., a chemical release or loss of traffic controls), theft of sensitive information that can be exploited, business interruption (e.g., denial of service), or other economic loss to the organization or its customers/users.

Example 1: The SCADA system performing water treatment operations at a water treatment facility.

Example 2: The traffic control operations system that manages transportation lights and cameras for a large city.

Example 3: The centralized network operations serving department and agency level IT services.

Example 4: The management system that handles medical records for a Health Information Exchange.

Example 5: The operations center that supports statewide law enforcement emergency management and coordination.

2.2 Comments and Briefing Notes

Blank areas have been provided for general comments. Consider briefing notes internal use only.. Briefing note areas are for short bullets that the *outbriefer* can use to quickly assemble the out-briefing and should only contain something that could be out-briefed to the facility.

Comment areas are for any comments that may be useful in QA or to explain a checkbox answer more fully. Consider comment areas available to all external users.

Critical Cyber Service (CCS) Information	
Service Name	_____
Other Service Names/Aliases	Alias: _____
Primary Systems Name	_____
Visit Date(s)	Start Date: _____ End Date: _____
Who Completed This Assessment?	☐ Resident CSA ☐ Non-resident CSA Name: _____ ☐ Other (e.g., SME) Name: _____
Is This a Multi-site Service?	☐ No ☐ Yes If yes, please describe: _____ If yes, indicate below which CCS location is being evaluated.
Street Address (City, County, State, ZIP Code, Country)	_____
Congressional District	_____
Latitude/Longitude *(Decimal format preferred)*	Latitude: _____ Longitude: _____
Assessment Motivation *(Check all that apply.)*	☐ Cyber Resilience Review ☐ RRAP ☐ Organization request ☐ Law enforcement request ☐ Direct threats/suspicious incidents: _____ ☐ Special event: _____ ☐ Other: _____

2.3 General Cyber Service Description (For Information Only)

The purpose of this list is to gather information on the organization's specific networks, services, applications, and connections to determine commonalities with other CCSs within the organization.

The purpose of these questions is to gather a general outline of what functions the CCS supports (e.g., Industrial Control, email, billing, or customer service Internet application) and what comprises the Service (e.g., hardware, software, devices, or workstations). Consider the "electronic security perimeter" for the Service, defined as the logical border surrounding a network to which critical cyber assets are connected and for which access is controlled (NERC glossary) and everything that is essential to the reliable operation of the Service. This will establish the CCS for which all other questions will be evaluated.

> For example, a SCADA Service may support the monitoring and control of the transmission of electric power within a specific geographic area, including redundant vendor servers, switches, and seven workstations in the company control center, fiber connections to 189 remote terminal units at substations, and limited connections to laptops and business servers, all operating on a specific vendor platform with in-house applications for power flow analysis and predictive planning.

For purposes of this survey the **cyber security budget** should be answered for the normal operations of the Service; not for unusual events or incident response staffing.

Critical Cyber Service (CCS) Information	
General CCS Description:	Check any that apply and provide a short description: ☐ Networks (wireless networks, wired networks, etc.): _____ _____ ____ ☐ Services (computer services, e-mail servers, web servers, control services, etc.): _____ _____ ____ ☐ Applications (computer programs, ERP software, shareware user-added non-company software, etc.): _____ _____ ____ ☐ Connections (VPN access by subcontractors, portable devices connected to organization services, interconnections between networks, connection of a CCS to the Internet, etc.): _____ _____ ____

Critical Cyber Service (CCS) Information	
Which of these cyber systems primarily defines the CCS? *(Check one.)*	☐ Business cyber system(s) that contain sensitive business information, whose exploitation could result in business interruption, economic loss, or theft. ☐ Business cyber system(s) that manage supply chain, inventory tracking, ordering and/or shipping, whose exploitation could result in the theft or diversion of property, business interruption, or economic loss. ☐ Business cyber systems that support business functions such as corporate email, payroll, human resources, reporting, scheduling, regulatory and other business-related functions, whose loss or exploitation could result in business interruption or economic loss. ☐ Internet cyber systems that support business functions, such as ordering, customer support, advertising, interactive business functions, and other business-related public interfaces, whose loss or exploitation could result in business interruption or economic loss. ☐ Cyber systems that perform physical security functions (e.g., physical intrusion detection services, access control services, camera services and monitoring software), whose loss or exploitation could result in security vulnerabilities, safety and health issues, damage to equipment or property, business interruption, or economic loss. ☐ Control system(s) that monitor and/or control on-site physical processes or manufacturing services, whose loss or exploitation could result in business interruption, safety and health issues, damage to equipment or property, or economic loss. ☐ Control system(s) that monitor and/or control remote physical processes or services, whose loss or exploitation could result in business interruption, safety and health issues, damage to equipment or property, or economic loss. ☐ Data storage system(s) that provide enterprise, backup, or archiving storage for the organization, whose loss could result in business interruption, theft, or economic loss. ☐ Data storage system(s) that provide enterprise, backup, archiving, or disaster recovery storage for others, whose loss could result in business interruption, theft, or economic loss. ☐ Other cyber system(s) whose exploitation could result in business interruption, safety and health issues, damage to property, or economic loss.

Critical Cyber Service (CCS) Information	
Which of the following cyber systems additionally comprise the primary CCS? *(Check all that apply.)*	☐ Business cyber system(s) that contain sensitive business information, whose exploitation could result in business interruption, economic loss, or theft. ☐ Business cyber system(s) that manage supply chain, inventory tracking, ordering and/or shipping, whose exploitation could result in the theft or diversion of property, business interruption, or economic loss. ☐ Business cyber systems that support business functions such as corporate email, payroll, human resources, reporting, scheduling, regulatory and other business-related functions, whose loss or exploitation could result in business interruption or economic loss. ☐ Internet cyber systems that support business functions, such as ordering, customer support, advertising, interactive business functions, and other business-related public interfaces, whose loss or exploitation could result in business interruption or economic loss. ☐ Cyber systems that monitor physical security of assets (e.g., intrusion detection services, access control services, camera services and monitoring software), whose loss or exploitation could result in security vulnerabilities, safety and health issues, damage to equipment or property, business interruption, or economic loss. ☐ Control system(s) that monitor and/or control on-site physical processes or manufacturing services, whose loss or exploitation could result in business interruption, safety and health issues, damage to equipment or property, or economic loss. ☐ Control system(s) that monitor and/or control remote physical processes or services, whose loss or exploitation could result in business interruption, safety and health issues, damage to equipment or property, or economic loss. ☐ Data storage system(s) that provide enterprise, backup, or archiving storage for the organization, whose loss could result in business interruption, theft, or economic loss. ☐ Data storage system(s) that provide enterprise, backup, archiving, or disaster recovery storage for others, whose loss could result in business interruption, theft, or economic loss. ☐ Other cyber system(s) whose exploitation could result in business interruption, safety and health issues, damage to property, or economic loss.
How many authorized users/customers have access to this CCS?	☐ 1 to 500 ☐ 501 to 5,000 ☐ 5,001 to 50,000 ☐ >50,000

Critical Cyber Service (CCS) Information				
What is the basis of the Cyber Security budget for this CCS?	☐ No formal budget is established	☐ Strict dollar amount	☐ Strict percentage of IT budget	☐ Strict percentage of overall budget

3.0 Cyber Security Management (LEVEL ONE)

For purposes of this evaluation cyber security management includes the leadership roles and responsibilities (e.g., governance), physical documentation, lifecycle tracking, information sharing (e.g., threat information), accreditation, assessment, and audits.

3.1 Cyber Security Leadership (LEVEL TWO)

Cyber security leadership includes roles and responsibilities (e.g., governance), physical documentation, lifecycle tracking, information sharing (e.g., threat information), accreditation, assessment, and audits.

Management may be deemed to a single individual or a department as long as roles and responsibilities are slated to cyber security.

Third-party contracts for cyber management or operational functions includes any/all cyber assessments, cyber documentation, IT audits, and/or additional work that is *not* done by the primary organization.

Cyber Security Leadership (LEVEL TWO)	
Is there a manager/department in charge of cyber security management?	☐ No ☐ Yes
If yes, is this the primary function of that manager?	☐ No ☐ Yes ☐ N/A
Is there a third-party contract arrangement for primary cyber management and/or operational functions for this CCS? <<Note: If answers to the above two questions are 'Yes,' the best answer here is 'No' .If answer to the first question above is 'No,' the best answer here is 'Yes.'	☐ No ☐ Yes If yes, describe what these responsibilities are: _____
Cyber Security Leadership Briefing Notes: _____	
Cyber Security Leadership Comments: _____	

3.2 Cyber Service Architecture (LEVEL TWO)

3.2.1 Cyber Service Inventory

A critical cyber asset inventory would include at minimum the network addresses, machine names, purpose of each Service and asset owner responsible for each device. It may also include every device with an IP address, including servers, desktops, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, VOIP, multi-homes addresses, virtual addresses, mobile phones, tablets, laptops, and other portable devices that store or process data.

Cyber asset — Programmable electronic devices and communication networks, including hardware, software and data. Data and cabling are considered to exist within the framework of the cyber asset and there are not separate cyber assets.

Network — Information Service(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Application — Application is digital application software program hosted by an information Service that functions and is operated by means of a computer, with the purpose of supporting functions needed by an asset owner.

Individuals – The key IT and security professionals within the organization. This would include: administrators, users, and third party contractors of the CCS.

For purposes of this evaluation, the review of inventory is the verification and validation of the cyber assets (networks, Services, applications, connections, and individuals). This process can be either manual (checking that the assets are physically there) or automated (computer system has inventory).

For this survey, an identified documented CCS asset security architecture should include all CCS cyber assets. The purpose of these questions are to document the security architecture's approval for additional assets into the architecture document and how frequently it is reviewed and updated.

3.2.2 Enterprise Architecture

A documented system architecture could include the following: routers, switches, computers, servers, firewalls, VPNs, remote desktops, virtual machines, networks, etc.

For the purpose of this survey, system configuration monitoring tools examples are: IBM Tivoli, IBM BigFix, Apache Subversion, & Perforce.

Cyber Service Architecture (LEVEL TWO)	
Inventory (LEVEL THREE)	
Is there an inventory of all critical cyber assets for this CCS?	☐ No ☐ Yes
If yes, does the inventory include *(Check all that apply.)*	☐ Networks (wireless networks, wired networks, etc.) ☐ Services (computer services, e-mail servers, web servers, control services, etc.) ☐ Applications (computer programs, ERP software, shareware user-added non-company software, etc.) ☐ Connections (VPN access by subcontractors, portable devices connected to organization services, interconnections between networks, connection of a CCS to the Internet, etc.) ☐ Individuals (e.g., key IT/IT security professionals, including administrators, users, and third-party vendors)
How frequently does the organization review its inventory?	☐ Never ☐ Upon change/continuous ☐ Annually ☐ Semiannually ☐ Quarterly ☐ At least monthly
Is there a documented security architecture that includes each of the identified CCS assets?	☐ No ☐ Yes
If yes, what protocol best represents what the organization employs to manage the security architecture with respect to asset changes? *(Check all that apply.)*	☐ Documented management approval for introduction of all new non-critical cyber assets ☐ Documented management approval for introduction of all new critical cyber assets ☐ Documented management approval for cyber security policy exceptions

If yes, does the document include any of the following? *(Check all that apply.)*	☐ Network Maps or Security Architecture Diagrams ☐ Network nodes/connections ☐ Interfaces/cyber service boundaries (e.g., the electronic perimeter) ☐ Traffic flows (network traffic patterns) ☐ Virtual Local Area Networks (VLANs) ☐ Software ☐ Work flows
How frequently does the organization re-evaluate its security architecture for coverage or inclusion of CCS assets?	☐ Never ☐ Upon change ☐ Annually ☐ Semiannually ☐ Quarterly ☐ At least monthly
Enterprise Architecture (LEVEL THREE)	
Is the system architecture or configuration documented?	☐ No ☐ Yes
If yes, how frequently does the organization review/update this architecture?	☐ Never ☐ Upon change ☐ Annually ☐ Semiannually ☐ Quarterly ☐ At least monthly
If yes, does the organization use system configuration monitoring tools that measure secure configuration elements and vulnerability information?	☐ No ☐ Yes

If yes, does the organization use system configuration management tools that will automatically enforce and redeploy configuration settings to services at scheduled intervals?	☐ No ☐ Yes
Cyber Service Architecture Notes: _____	
Cyber Service Architecture Comments: _____	

3.3 Change Management (LEVEL TWO)

3.3.1 Change Management

Change management is the control procedures required to change the baseline configuration of a Service. The baseline configuration is the set of specifications for a Service that has been formally reviewed and agreed on at a given point in time and can be changed only through formal change procedures. Configuration controls include controlling modifications to hardware, firmware, software, and documentation to protect the information Service against improper modifications prior to, during and after Service implementation.

Change Management	
Which option best describes the organization's approach to cyber change management (e.g., new hardware/software, employee access)? *(Check one.)*	☐ Has revision logs documenting who made the changes to a policy, procedure, plan, inventory or architecture documentation and incorporating a brief synopsis of the change and the corresponding date of those changes; this would include a backout plan. ☐ Has a documented and distributed cyber change management policy and supporting procedures. ☐ Has documented and distributed change management procedures. ☐ Has an ad hoc process for regulating and approving changes. ☐ Does not do change management.
Does the organization use software distribution restrictions (e.g., "white listing technology") to identify approved software that can be installed on the CCS?	☐ No ☐ Yes If yes, how frequently is the list updated? ☐ Never ☐ Upon change ☐ Annually ☐ Semiannually ☐ Quarterly ☐ At least monthly
Does the Service have a standard for configurations of software to include operating systems?	☐ No ☐ Yes

What measures does the organization employ to manage the configuration of this CCS? *(Check all that apply.)*	☐ Identifies all hardware and disables all unnecessary elements ☐ Identifies all software and disables all unnecessary elements ☐ Identifies all sensitive information ☐ Identifies all services and disables all unnecessary elements ☐ Identifies security vulnerabilities ☐ Identifies and mitigates security vulnerabilities by implementing compensating security controls (e.g. offline) ☐ Strictly defines standardized service configurations ☐ Identifies and addresses non-compliant configurations ☐ Identifies all network communication devices, media, and means and ensures they have appropriate cyber security controls in place.
Change Management Briefing Notes: _____	
Change Management Comments: _____	

3.4 Lifecycle Tracking (LEVEL TWO)

For purposes of this evaluation, a life cycle is defined in the phases of which it passes through initiation, development, operation, and termination.

For purposes of this evaluation, third party vendors and service providers would be any organization outside the evaluated facility that provides service or products to the evaluated facility. (e.g. software, hardware, electricity, water)

The question set referring to procurement and contracting measures refers to the needs of third-party vendor contracts to address certain security requirements and who has oversight of the contracts.

A system that are not or cannot be updated with respect to critical vulnerabilities would be mean: outdated operating system or a business reason – break hardware or software doesn't work.

Proof of cyber security integration into the CCS asset life cycle can be done with certifications, operation plans, implementation procedures, and policies.

Lifecycle Tracking	
Does the organization employ measures to address the security of CCS assets throughout their life cycle (inception through disposal)?	☐ No ☐ Yes
Does the organization employ procurement and contracting measures to specify and enforce security requirements for third-party service providers and vendors? (if applicable)	☐ No ☐ Yes ☐ N/A
If yes, which approach best describes the procurement and contracting measures? *(Check one.)* **Amanda – moved around for proper order*	☐ The organization has a policy that requires third-party agreements to address security requirements, but does not specify security standards. The management and oversight of security is informal and reactive. ☐ The policy specifies standards outlining security requirements for third-party contracts, using pro-forma, boiler-plate language. The management and oversight of third-party compliance with standards is informal. ☐ The organization monitors, reviews, and requires third-party compliance with security standards. Management requires ongoing demonstrated compliance with standards before continuing or awarding contracts. Assessments of risks are discussed in ongoing conversations between partners. ☐ The organization assigns security professionals to review and oversee third-party adherence to security requirements The vendor periodically reports on their performance towards the security requirements. This third party requirement is uniformly practiced between most third parties and the organization, and all exceptions are documented.
Which approach best describes the cyber security policy in the organization's CCS asset life cycle? *(Check one.)*	☐ Organization integrates cyber security into the CCS asset life cycle (design, procurement, installation, operation, and disposal). ☐ Organization establishes security requirements for all CCS assets and networks before they are put into operation, and for all operational services and networks throughout their life cycle. ☐ Organization establishes security requirements for all CCS security assets and networks before they are put into operation, and manages those requirements through change and vulnerability management for all critical operational services and networks throughout their life cycle.
Does the organization employ any of the following security controls to prevent	☐ Organization routinely identifies available software security patches and updates.

malicious code from exploiting the CCS?	☐ Organization applies appropriate patches and updates to systems as soon as possible, given critical operational and testing requirements.
Approximately what percentage of CCS systems are not or cannot be updated with respect to critical vulnerabilities? (e.g. outdated or business reason – break software)	☐ 75% or more ☐ ≥ 50% but less than 75% ☐ ≥ 25% but less than 50% ☐ ≥ 10% but less than 25% ☐ less than 10%
If the organization has CCS systems that are not or cannot be updated with respect to critical vulnerabilities, approximately what percentage of these systems have compensating security controls in place?	☐ 100% ☐ ≥ 75% but less than 100% ☐ ≥ 50% but less than 75% ☐ ≥ 25% but less than 50% ☐ ≥ 10% but less than 25% ☐ less than 10%
Which documents does the organization retain that can demonstrate integration of cyber security into the CCS asset life cycle? *(Check all that apply.)*	☐ Security accreditation/certification ☐ Requirements analysis ☐ Acquisition plans and/or procedures ☐ Implementation plans and/or procedures ☐ Operations plans and/or procedures ☐ Change management plans and/or procedures ☐ Vulnerability management plans and/or procedures
Lifecycle Tracking Briefing Notes: _____	
Lifecycle Tracking Comments: _____	

3.5 Accreditation and Assessment (LEVEL TWO)

Does the facility utilize formal, external cyber-security guidance and standards for identifying and implementing cyber-security controls (management, operational, and technical)?The purpose of capturing accreditation and assessment information is to see if the facility utilizes external standards to develop policies regarding cyber security including policies that affect people, processes, and equipment. This information is to help to compare across sectors and amongst different standards.

The purpose of capturing if an audit or assessment is conducted in accordance with the standard practiced is to benchmark the particular standards and their practiced requirements.

Accreditation and Assessment	
Does your organization follow a cyber security standard(s) of practice? Not scored—information only.	☐ No ☐ Yes If yes, which standard(s) of practice do you follow? *(Check all that apply.)* ☐ NIST SP 800 Series ☐ ISO/IEC 27000 Series ☐ CObit ☐ ITIL ☐ HITRUST ☐ ISF Standard of Good Practice (SOGP) ☐ NERC CIP ☐ FIPS 199 ☐ HIPAA ☐ NIST Cyber Security Framework ☐ Other_____ <<Suggestion from panel member add: Canada PEPIDA/European Safe Harbor>>
If yes, a standard of accreditation is required for: *(Check all that apply.)* Not scored—information only.	☐ Business requirements ☐ Legislative or regulatory requirements ☐ Contractual requirements ☐ Organization policy
If yes, is audit required against the standards? Not scored—information only.	☐ No ☐ Yes
Does the organization conduct cyber security vulnerability/risk assessments to identify potential	☐ No ☐ Yes

vulnerabilities of the CCS assets and networks? <<Suggestion that the question delete 'risk' and only refer to vulnerability assessments.	
If yes, is this done to meet the standard of accreditation required above? Not scored—information only.	☐ No ☐ Yes
If yes, how often does the organization conduct these assessments? *(Check one.)*	☐ Monthly ☐ Quarterly ☐ Annually ☐ Every two years ☐ More than two years between assessments
In what ways are the CCS assets assessed? *(Check all that apply.)*	☐ Internal vulnerability testing ☐ External vulnerability testing ☐ Internal vulnerability and penetration testing ☐ External vulnerability and penetration testing ☐ Documentation review (tabletop) ☐ Manual checklist
Are cyber security assessment results reported to a broader segment of senior management than IT Security?	☐ No ☐ Yes If yes, describe how: _____
Accreditation and Assessment Briefing Notes: _____	
Accreditation and Assessment Comments: _____	

3.6 Cyber Security Plan (LEVEL TWO)

Organizations must develop, document, update, and implement: the security plans or the planned security plans for organizational information Services that describe the security controls to be in place and the rules of behavior for individuals accessing the information Services.

3.6.1 Does the Organization have a Cyber Security Plan?

The best answer to this question should be "YES" if the facility has documentation that addresses cyber security or cyber service continuity. A cyber service involves addressing continuity of operations, business continuity, cyber disaster recovery, etc. These plans may exist separately or could be included in the organizations overall plans but should address cyber specifically.

3.6.2 Are Personnel Trained on the Plan?

The intent of this question is to capture if the personnel know the plan and its content (procedures), and their role in the case of an incident. They should be well versed with this material and have regular refresher courses.

Cyber Security Plan (LEVEL TWO)	
Is there a Cyber Security Plan covering this CCS?	☐ No ☐ Yes If yes, The plan is developed at the (Check all that apply): ☐ Management level (e.g. managers, senior management) ☐ Operational unit level (e.g. IT administrators) ☐ Service level (e.g. users) Has the plan been approved by a broader segment of senior management than IT Security? ☐ No ☐ Yes Does a Federal, state, or local regulation or organizational policy require the plan? ☐ No ☐ Yes Are key cyber personnel aware of, trained on, and have access to a copy of the plan? ☐ No ☐ Yes
Does the Cyber Security Plan address: *(Check all that apply.)*	☐ Identification and classification of critical cyber services/assets ☐ Access control policies ☐ Cyber security roles and responsibilities ☐ Cyber security training ☐ Audit trails ☐ Disposal of protected assets ☐ Security/vulnerability testing ☐ Cyber security awareness ☐ Security Event Monitoring ☐ Physical security of critical cyber services/assets

	☐ Firewalls ☐ Electronic communications ☐ Mobile devices ☐ Media ☐ Remote access ☐ Wireless access ☐ Security patches or updates ☐ Incident Response/Management ☐ Unauthorized access ☐ Denial of service ☐ Malicious code ☐ Improper usage ☐ Scans/probes/attempted access ☐ Disaster recovery ☐ Data backup and recovery ☐ Availability of alternative site ☐ None of the above

On what basis is the plan reviewed and revised? *(Check all that apply.)*	☐ Never ☐ After incidents ☐ Upon introduction of new regulations ☐ After business changes ☐ Upon major operational environment changes ☐ Annually
Cyber Security Plan Briefing Notes: _____	
Cyber Security Plan Comments: _____	

3.7 Cyber Security Exercises (LEVEL TWO)

For purposes of the cyber security exercise questions, if none of the suggested purposes provided are marked, it is assumed that cyber security exercises are done for compliance reasons only.

For purposes of this evaluation, the distinction between tabletop, functional, and full scale exercises are as follows:
Tabletop - practical or simulated exercise typically talked about but not executed in production.
Functional - specialized exercise typically in a specific area that can be an isolated event
Full scale - simulated or actual event typically consuming the entire organization to practice

Cyber Security Exercises (LEVEL TWO)	
Does the organization conduct cyber security exercises?	☐ No ☐ Yes If yes, for what purpose(s)? *Check all that apply.]* ☐ Cyber awareness ☐ Service testing ☐ Continuity planning ☐ Disaster recovery ☐ Incident preparedness ☐ Threat and incident coordination ☐ Partner readiness If yes, these exercises are: ☐ Tabletop without external participants (practical or simulated exercise) ☐ Tabletop with external participants (e.g., vendors, cyber contractors, regulatory agencies, or CIP providers) ☐ Functional without external participants (specialized exercise) ☐ Functional with external participants (e.g., vendors, cyber contractors, regulatory agencies, or CIP providers) ☐ Full scale without external participants (simulated or actual event) ☐ Full scale with external participants (e.g., vendors, cyber contractors, regulatory agencies, or CIP providers) If yes, how often are exercises conducted? ☐ Greater than one year ☐ Annually ☐ Semiannually ☐ Quarterly ☐ Monthly If yes, are exercise results documented, approved and reported to a broader segment of senior management than IT Security? ☐ No ☐ Yes

3.8 Information Sharing (LEVEL TWO)

3.8.1 Does the Facility Report Cyber-Security Incidents to Outside Organization?

Organizations have varying criteria for declaring a cyber security incident. However, in general terms, a cyber security incident is an event that violates written or implied security policies. Depending on the organization, examples might include spear phishing campaigns, stolen data, and denial service attacks.

The purpose of validation back to the organization is to allow for better reporting standards. A "Yes" answer means the organization refers back to the document owner providing some feedback that this information was helpful or not to them. A "No" answer means the organization does not give any feedback to originating organization.

3.8.2 Does the Organization Notify or Communicate Security Information to Personnel?

A "No" response means that no security information is communicated to company personnel (e.g., no additional information other than emergency plan information - evacuation or fire drill information). Specific security incident information is for an actual security incident (e.g., suspicious people have been observed around the organization back doors, a change in NTAS level, or how to thwart known attempts at hacking the company cyber servers).

External Information Sharing (LEVEL THREE)	
Does the organization receive threat information, cyber-security-related bulletins, advisories, and/or alerts from an external source?	☐ No ☐ Yes If yes, from whom? ☐ DHS entities ☐ FBI entities ☐ Vendors/industry Which one(s)? _____ Is it sector-based (e.g. Industry ISACs)? ☐ No ☐ Yes ☐ State or local law enforcement department(s) ☐ Fusion Centers ☐ Other Which one(s)? _____ If yes, how often does the organization receive and process this information? ☐ Monthly ☐ Weekly ☐ Daily/Continuously If yes, does the organization provide any feedback or validation to the originating organization? ☐ No ☐ Yes
Does the organization receive vulnerability information, cyber-security-related bulletins, advisories, and/or alerts from an external source?	☐ No ☐ Yes If yes, from whom? ☐ DHS entities ☐ FBI entities ☐ Vendors/industry Which one(s)? _____ Is it sector based (e.g. Industry ISACs)? ☐ No ☐ Yes ☐ State or local law enforcement department(s) ☐ Fusion Centers ☐ Other Which one(s)? _____

External Information Sharing (LEVEL THREE)	
	If yes, how often do you receive and process this information? ☐ Monthly ☐ Weekly ☐ Daily/Continuously If yes, does the organization provide any feedback or validation to the originating organization? ☐ No ☐ Yes
Does the organization report cyber-security incidents to outside organizations?	☐ No ☐ Yes If yes, for what purpose(s) do you make such reports? *(Check all that apply.) Not scored—information only.* ☐ Request technical assistance (U.S. CERT, IRT teams, etc.) ☐ Request incident management support ☐ Regulatory (e.g., NERC CIP) ☐ Information sharing (e.g., U.S. Cert, state computer security incident response teams, fusion centers) ☐ Law enforcement (e.g., FBI, USSS, state/local police) Describe: _____
Does the organization share cyber-security information with outside organizations?	☐ No ☐ Yes If yes, what information is shared? ☐ Suspicious-activity reports ☐ Threat analysis ☐ Vulnerability analysis ☐ Subset of information reporting ☐ Confirmed incidents ☐ Status and configuration of security controls
Does anyone from the organization actively participate in local or regional cyber security forums (e.g., exchange of lessons learned, best practices, training)?	☐ No ☐ Yes If yes, please list and describe. ☐ Sector-specific information sharing and analysis centers Which one(s)? _____ ☐ Sector-related associations/partnerships Which one(s)? _____

External Information Sharing (LEVEL THREE)	
	☐ Federal or State-led partnerships (e.g., FBI InfraGard chapter[s]) Which ones? _____ ☐ Fusion center(s) Which one(s)? _____ ☐ State or local law enforcement department(s) Which one(s)? _____ ☐ Federal law enforcement department(s) Which one(s)? _____ ☐ State or local cyber office(s) Which one(s)? _____ ☐ Other(s) Describe: _____

Internal Information Sharing (LEVEL THREE)	
Does the organization notify or communicate cyber security information to personnel?	☐ No ☐ Yes If yes, what type of personnel? *(Check all that apply.)* ☐ Corporate officers ☐ Cyber teams/Incident Management teams ☐ Managers ☐ Users If yes, what type of information? (*Check all that apply.)* ☐ Specific security incident information ☐ General security awareness ☐ Crisis and emergency information ☐ Threat information What methods are used to communicate? *(Check all that apply.)* ☐ Recurring meetings ☐ Email communications ☐ Web-based training ☐ Phone communications For what purpose? *(Check all that apply.)* ☐ To build a common operating procedure ☐ For security awareness

Internal Information Sharing (LEVEL THREE)	
	☐ Other: _____ Describe: _____

Information Sharing Briefing Notes: _____
Information Sharing Comments: _____

4 Cyber Security Forces (LEVEL ONE)

4.1 Personnel (LEVEL TWO)

Make a note about the positions

4.1.1 Are Background Checks Conducted?

It is understood that there may be limitations to background checks in some states or for foreign contractors. The intent of the question is to determine if there is a process for background checks. Often background checks are a reasonable action to dissuade insider threats or to ensure effective hiring practices. If foreign contractors do not have background checks, but are allowed to be in the facility without restrictions, then do not select contractors/support functions.

Personnel	
Are the following positions formalized within your organization? *(Check all that apply.)*	☐ Cyber Security Policy and Planning Coordinator ☐ Cyber Security Training Official ☐ Cyber Security Incident Response Team Lead/Incident Commander ☐ CERT Staff/Triage Staff (Incident Responder) ☐ Cyber Security Exercise Official ☐ Security Operations Personnel (i.e., Security Administrators, Security Analysts) ☐ Cyber Security Threat Coordinator ☐ IT Controls and Compliance Staff ☐ Security Architect ☐ Application Administrator
Do you have a policy that authorizes and holds accountable the personnel having these assignments?	☐ No ☐ Yes ☐ N/A
Are background checks conducted for organizational and supporting personnel?	☐ No ☐ Yes If yes, on whom are background checks conducted? Organizational cyber security personnel ☐ No ☐ Yes If yes, are recurring background checks conducted? ☐ No ☐ Yes Contract cyber security personnel ☐ N/A ☐ No ☐ Yes If yes, are recurring background checks conducted? ☐ No ☐ Yes Cyber vendors ☐ N/A

	☐ No ☐ Yes If yes, are recurring background checks conducted? ☐ No ☐ Yes

4.2 Cyber Security Training (LEVEL TWO)

Cyber security training has become policy in most organizations but the standards used are different among each organization. This cyber security training question set is here to understand what the median is for type, frequency, and purpose of these training program practices.

Training (LEVEL TWO)	
Do cyber security personnel involved in day-to-day operations receive cyber training?	☐ No ☐ Yes If yes, Training programs are: *(Check all that apply)* ☐ Industry-recognized certification ☐ Formal ☐ In-house/informal ☐ Video ☐ Web-based ☐ OJT (on-the-job training) Frequency of continuation/refresher training: ☐ Never ☐ Annually ☐ Semiannually ☐ Quarterly ☐ Monthly ☐ Weekly Are personnel formally trained in the following areas? *(Check all that apply.)* ☐ Business continuity/disaster recovery ☐ Training (e.g., user training, train-the-trainer) ☐ Server administration ☐ Network administration ☐ Contingency ☐ Threat analysis ☐ Risk management If yes, how often? ☐ Only following an incident ☐ Greater than one year ☐ Annually ☐ Semiannually ☐ Quarterly ☐ Monthly
Are cyber personnel trained on the cyber security plan?	☐ No ☐ Yes

Has the organization established and documented a minimum level of training, education and/or experience required for cyber security personnel?	☐ No ☐ Yes If yes, how is fulfillment of the requirement(s) evidenced? *(Check all that apply.)* ☐ Current professional certification ☐ Information security degree ☐ Previous work experience ☐ Position description and/or performance monitoring ☐ Human resources file of professional development and performance management
Does the organization track the training as part of the performance monitoring process?	☐ No ☐ Yes
Training Briefing Notes: _____	
Training Comments: _____	

5 Cyber Security Controls (LEVEL ONE)

5.1 Identification, Authentication, and Authorization Controls (LEVEL TWO)

The purpose of this question set is to find the basis of authentication and authorization controls used on the CCS within the evaluated organization. Common practices such as administrator privileges, user privileges, and password management are assessed.

For purposes of this evaluation, identity proofing is divided into 5 categories: risk-based, controls-based, best-practices, vendor-based, some other basis.

Risk-based is a non-static authentication system which takes into account the profile of a user requesting access to system. An example is asking additional security question if they login from a different computer or IP.

Controls-based is an approach that restricts system access to authorized users. This means that users have to authenticate based on their roles and they are only deemed their privileges based off what they need.

Best-practices is an example of authentication such as two-step verification. Using RSA keys and Cryptocards are examples of second steps of verification. Another example is that DISA produces a STIG and most government institutions follow that STIG.

Vendor-based example is: Microsoft recommends that a virus scanner is needed.

The term “Some other basis” will be the catch all.

Identification, Authentication, and Authorization Controls (LEVEL TWO)	
Has the organization established a process for identity proofing and authentication to limit access to the CCS to only authorized persons?	☐ No ☐ Yes
If yes, what is the basis for establishing identity proofing and authentication? (Check all that apply.)	☐ Risk-based ☐ Controls-based ☐ Best-practice-based e.g., RSA ☐ Vendor-based ☐ Some other basis (e.g. management judgment)
If yes, for whom has the organization implemented these specific identity proofing and authentication processes? (Check all that apply.)	☐ CCS users ☐ Administrators ☐ Contractors (if applicable) ☐ Vendors (if applicable)
Does the organization practice the concept of least privileges (i.e., users are only granted access to the information, files, and applications required to fulfill their roles and responsibilities)?	☐ No ☐ Yes
If yes, which of the following measures does the organization employ to control least privileges? *(Check all that apply.)*	☐ Access control list based upon information available, confidentiality and integrity requirements. ☐ Access control list based upon functional isolation requirements. ☐ Data loss prevention technology. ☐ Management review of access privileges per level at least annually. ☐ All user accounts have an expiration date. ☐ All user accounts are audited and event logged. ☐ Accounts are unique to individuals or functions. ☐ An established functional or business requirement. ☐ Rights can be temporarily suspended.

If yes, which of the following measures does the organization employ to control administrator privileges? *(Check all that apply.)*	☐ Rights are granted on a temporary basis for specific functions. ☐ All user accounts with administrator privileges are approved by management. ☐ All users with administrator privileges are trained on cyber security requirements. ☐ All accounts with administrative-level access are centrally logged and audited.
Is username/password the primary means of user authentication to the CCS? *(Check only one.)*	☐ Yes ☐ No
If yes, which of the following password management policies are implemented for the CCS? *(Check all that apply.)*	☐ Organization enforces a complexity and length requirement on the password. ☐ Organization enforces a reuse policy on passwords forbidding the use of recently used of passwords. ☐ Organization enforces 1 time hashed based passwords. ☐ Organization disallows shared passwords forcing each user and service to have its own username/password. ☐ No password management policies exist
What additional properties of authentication are employed for the critical cyber service?	☐ Central notification/logging of failed logins ☐ Additional layers of authentication (e.g., sequential) ☐ Account lock-out (after a defined number of failures) ☐ Unique forms of authentication (includes multiple-factors)
If the primary means of authentication failed, has the organization determined that compensating controls would provide sufficient authentication?	☐ No ☐ Yes
Does the organization have a protocol for removing, suspending or modifying user accounts upon change of employment?	☐ No ☐ Yes
If yes, when is a user account modified,	<<Suggestion for future: De-activated or deleted **prior to the organization notifying the user** of an adverse human resources action

deleted, or de-activated? *Amanda – switched for proper order	☐ De-activated or deleted no later than close of business on the day when organization notifies user of an adverse human resources action (e.g. being fired, layoff) ☐ De-activated or deleted no later than close of business on the day when user leaves organization as a result of an adverse human resources action (e.g. being fired) ☐ De-activated or deleted more than one business day after user leaves organization as a result of an adverse human resources action ☐ De-activated or deleted no later than one week after user leaves organization ☐ De-activated or deleted more than one week after user leaves organization ☐ Modified no later than one business day after user notifies the organization of a change in role ☐ Modified no later than one business day after user transfers into new role ☐ Modified no later than one week after user transfers into new role ☐ Modified more than one week after user transfers into new role
Does the organization have a protocol for monitoring user activity after changes in employment related to termination?	☐ No ☐ Yes Does the organization monitor user activity following notification of employee change up to termination? ☐ No ☐ Yes Does the organization monitor user activity following employee termination? ☐ No ☐ Yes Does the organization review historic activity for a period of time prior to the notification? ☐ No ☐ Yes
Identification and Authentication Briefing Notes: _____	
Identification and Authentication Comments: _____	

5.2 Access Controls (Level Two)

5.2.1 Unauthorized Access

An individual gains logical or physical access without permission to a network, Service, application, data, or other resource.

5.2.5 Remote Access

Remote Access allows connectivity to the internal network from the outside. User controls can include only allowing designated users to connect remotely, vs. all users; use of secure tokens; changing default passwords on remote devices; etc.

Access Control (LEVEL TWO)	
Access Paths (LEVEL THREE)	
Has the organization established a business requirement for every access path to/from the CCS?	☐ No ☐ Yes
Does the organization implement security controls to limit access across the documented boundaries (e.g., firewalls, IDS port security, or rules of behavior)?	☐ No ☐ Yes
If yes, does the CCS benefit from access control device(s) that restrict incoming and/or outgoing connections between the CCS and the Internet? (Check all that apply.)	☐ CCS benefits from access control device(s) that restrict incoming Internet connections. ☐ CCS benefits from access control device(s) that restrict outgoing Internet connections.
If yes and applicable, does the CCS benefit from access control device(s) that restrict incoming and/or outgoing connections between the CCS and a non-critical system that is connected to the Internet? (Check all that apply.)	☐ CCS benefits from firewall(s) that restrict incoming connections to critical systems. ☐ CCS benefits from firewall(s) that restrict outgoing connections from critical systems.
Which of the following security measures does the organization employ for preventing exploitation of access paths? *(Check all that apply.)*	☐ Inspection of inbound data communications ☐ Inspection of outbound data communications ☐ Policy- or rule-based data communications filtering/blocking ☐ External source/destination filtering ☐ Portable storage device/media data communications controls ☐ Detection and/or controls of unmanaged devices (non-organization-owned laptops, smartphones, etc.)
Remote Access Controls (LEVEL THREE)	
Does the organization allow remote access to critical cyber services/assets? (No is best answer.)	☐ No ☐ Yes

Which of the following measures does the organization employ to control remote access to the organization's cyber services?	☐ Terms-of-use policies regarding user responsibilities and expected behavior ☐ Terms-of-use policies regarding service usage ☐ Terms-of-use policies regarding allowed and/or prohibited activities ☐ Access allowed only when needed, requested and authorized but disabled otherwise ☐ Remote-client filtering ☐ Multi-factor authentication ☐ Mandatory communications encryption ☐ Multiple session controls ☐ Session monitoring ☐ Session timeout
Access Controls Briefing Notes: _____	
Access Controls Comments: _____	

5.3 Cyber Security Measures (LEVEL TWO)

5.2.3 Malicious Code

Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating Service or application.

5.2.x Improper usage:

a person violates acceptable computing use policies.

EVENT LOGGING: For purposes of this evaluation, event logging is log retention of services such as networks, endpoints, applications, etc.

Monitoring and Scanning (LEVEL THREE)	
Which of the following cyber security measures does the organization employ for monitoring of networks related to the CCS? *(Check all that apply.)*	☐ Near-real-time monitoring for malicious code ☐ Near-real-time monitoring for unauthorized access ☐ Near-real-time monitoring for unauthorized software ☐ Near-real-time network boundary intrusion detection ☐ Near-real-time network boundary traffic monitoring ☐ Near-real-time host intrusion monitoring ☐ Automated security event response and alerting ☐ Automated security event alerting ☐ Manual, non-real-time network monitoring based on audit logs
For what purpose does the organization perform monitoring? *(Check all that apply.)*	☐ Problem identification ☐ Performance monitoring ☐ Configuration control ☐ Data Loss monitoring ☐ Threat monitoring
Malicious Code Controls (LEVEL THREE)	
Does the organization employ any of the following security controls to prevent malicious code from exploiting the CCS? *(Check all that apply.)*	☐ Up-to-date real-time, host-based anti-virus/malware software to prevent malicious code from exploiting CCSs ☐ Signature-based ☐ Heuristics-based ☐ Anomaly-based ☐ Network- or gateway-based malware scanning to prevent malicious code from exploiting CCSs ☐ Signature-based ☐ Heuristics-based ☐ Anomaly-based
Security and Event Log (LEVEL THREE)	
Does the organization maintain security and event logs?	☐ No ☐ Yes If yes, ☐ There is a log retention policy. ☐ Logs are maintained in a standardized format. ☐ Logs are archived.
Are logs reviewed for anomalies either in a	☐ No ☐ Yes

manual or automated fashion?	
What types of logs are *manually* reviewed for unauthorized activities? (Check all that apply.)	☐ Services (network daemons, etc.) ☐ Applications ☐ Firewall logs ☐ Communication devices, e.g., routers and switches ☐ Servers ☐ Endpoint devices ☐ No service logs are reviewed by operators. ☐ Other: _____
What types of logs are *automatically* reviewed for unauthorized activities? *(Check all that apply.)*	☐ Services (network daemons, etc.) ☐ Applications ☐ Firewall logs ☐ Communication devices, e.g., routers and switches ☐ Servers ☐ Endpoint devices. ☐ No service logs are reviewed ☐ Other: _____
What is the *manual* review frequency for each type of log indicated above? *(Check one.)*	☐ Greater than one year ☐ Annually ☐ Semiannually ☐ Quarterly ☐ Monthly ☐ Weekly ☐ Daily
What is the *automatic* review frequency for each type of log	☐ Weekly

indicated above? (Check one.)	☐ Daily ☐ Continuous
Are logs correlated with scans, assessments, audits, and other security controls?	☐ No ☐ Yes If yes, describe how: _____
Are reports generated from anomalies identified in logs?	☐ No ☐ Yes If yes, describe how: _____
Monitoring and Scanning Briefing Notes: _____	
Monitoring and Scanning Comments: _____	

5.4 Information Protection (LEVEL TWO)

INFORMATION PROTECTION (SENSITIVE INFO): For purposes of this evaluation, information protection for sensitive information is sought to find out that it is identified and properly managed.

Information Protection	
Is sensitive information (e.g., network diagrams, CCS inventories) identified and categorized?	☐ No ☐ Yes
How is sensitive information managed? *(Check all that apply.)*	☐ Secure storage (Encrypted while at rest) ☐ Limited access (password-protected) ☐ Role-based access ☐ Adequately destroyed (e.g., e-shredding, secure delete) ☐ Protective markings ☐ Secure transmission (encrypted in flight) ☐ Archived and/or backed up
If sensitive information is archived and/or backed up offline, how often are backups performed?	☐ Monthly ☐ Weekly ☐ Daily
Is real-time replication occurring to a different site or piece of hardware?	☐ No ☐ Yes
If sensitive information is archived and/or backed up, are data restores performed and verified (e.g., are backup data restored and checked to see if they work)?	☐ No ☐ Yes
Is there a security review before information is released outside of operations (partner sharing, public release, etc.)?	☐ No ☐ Yes
Information Protection Briefing Notes: _____	

Information Protection Comments: _____

5.5 User Training (LEVEL TWO)

USER TRAINING: The purpose of these questions in this section is not to find out what type of training but to find out when the user is trained and when the user receives access to network.

Does the organization provide training on cyber security for CCS users?	☐ No ☐ Yes If yes, how often? ☐ Only following an incident ☐ Greater than one year ☐ Annually ☐ Semiannually ☐ Quarterly ☐ Monthly
If yes, when does the organization provide cyber security training?	☐ Before the user obtains access ☐ Within 1 week of obtaining access ☐ Within 30 days of obtaining access ☐ More than 30 days after obtaining access ☐ As remediation upon security violations or other infractions ☐ Training is incidental to a lessons-learned process
If yes, which of the following topics is included in CCS user training? *(Check all that apply.)*	☐ General review of organization's cyber policies ☐ Review of organization's cyber security policies ☐ User roles and responsibilities ☐ Password procedures ☐ Acceptable usage practices ☐ Identification and reporting of incidents and suspicious activities ☐ Cyber security situational awareness and best practices ☐ Cyber security threats, trends and attacks
User Training Briefing Notes: _____	
User Training Comments: _____	

5.6 Defense Sophistication and Compensating Controls (LEVEL TWO)

DEFENSE SOPHISTICATION/ COMPENSATING CONTROLS: for purposes of this evaluation best judgment is to be used for defense sophistication/compensating controls. Examples of this are moving target defense, diverse platforms, etc.

Defense Sophistication and Compensating Controls	
Does your organization employ additional advanced tactics, strategies and/or specific layered defenses to compensate for a loss of primary controls? (Examples may include platform diversity, moving-target defense, etc.)	☐ No ☐ Yes If yes, describe: _____

6.0 Incident Response (LEVEL ONE)

6.1 Incident Response Measures (LEVEL TWO)

6.1.1 Incident Response/Management

For purposes of this evaluation, an incident response plan should be documented in its full form. It should be agreed on and signed off by all officials. All personnel should know the plan and be fully aware of it. This incident response plan should contain items of how to respond to incidents, emergencies, and smaller events. It should layout key plans that the organization has practiced in case of an incident.

6.1.3 Does the facility participate in provider priority plan for restoration?

A priority plan is a "list" of facilities or types of facilities that will be restored before other types of facilities. For instance, most utilities will prioritize human health facilities such as hospitals, water treatment Service assets, and nursing homes and restore service to them before other customers.

Incident Response Measures	
Does the organization have predefined plans for responding to cyber security incidents?	☐ No ☐ Yes
The organization has a defined incident response plan for handling cyber incidents, which (at a minimum) contains: *(Check one.)*	☐ Documented procedures, security violations and conditions, and assigned roles for cyber security incident response ☐ Assigned roles for cyber security incident response but no documented procedures ☐ No assigned roles for cyber security incident response and no documented procedures
The organization has defined incident response procedures for handling cyber incidents, which (at a minimum) contain: *(Check all that apply.)*	☐ Planned procedures for network containment ☐ Planned procedures for malware containment(s) and boxing ☐ Planned procedures to rate limit in response to a Distributed Denial of Service attack ☐ Planned procedures to respond to an unauthorized access to sensitive information ☐ No incident response procedure exists.
How often do you test cyber-incident response procedures/capabilities (Continuity of Operations Plans, Disaster Recovery Plans, Business Continuity Plans, etc.)?	☐ Never ☐ Every two years ☐ Annually ☐ More than once a year
How do you test cyber-incident response procedures/capabilities (Continuity of Operations Plans, Disaster Recovery Plans, Business Continuity Plans, etc.)?	☐ With a controlled live-fire incident chosen by an outside source ☐ With a controlled live-fire incident chosen by an inside source ☐ With a tabletop exercise ☐ Via document review
How often do you review responses to actual cyber incidents to see if they are consistent with the incident response procedures/plan (Continuity of Operations Plans, Disaster Recovery	☐ Within a reasonable time after incident resolution, as part of follow-on actions ☐ Monthly ☐ Semiannually ☐ Annually

Plans, Business Continuity Plans, etc.)?	☐ Never
Is there a written contract with entities other than emergency responders (e.g. other organizations, other companies, contract response companies, water and wastewater agency response networks)?	☐ No ☐ Yes

Incident Response Measures Briefing Notes: _____
Incident Response Measures Comments:

6.2 Alternate Site and Disaster Recovery (LEVEL TWO)

For purposes of this evaluation, *severely impacted* means that the organization is running at a level considered "significantly lower output to no output" of work.

6.2.1 Is There Alternate Site for Continuity of Business?

Key features of an alternate site include its characterization and the percent of the normal level of the main facility's production it can handle.

This would be the core operations are moved to an alternative site. For instance, the data control center can operate from another data control center in another city; that is an alternative site. If a team can play in another stadium (e.g., when the Bears played at the University of Illinois while their stadium was being modified), that is another example of an alternate site. However, the fact that people can shop at an alternate mall is not an alternate site for the facility being assessed. The fact that there are other hotels in the area is not an alternate site. Also, if the only thing that has an alternate site is the data center and all other core functions cease, then perhaps it is not an alternate site. If the core mission is carried out remotely from employee's homes, for instance, that is not an alternate site. Facilities like manufacturing, hospitals, hotels, malls, bridges, tunnels, stadiums, arenas, racetracks, casinos, most general office buildings and similar facilities rarely have an alternate site. Data centers, government agencies / functions, banking and communication facilities often have an alternate site. For instance, redundant data centers where data is backed up but operating terminals would have to be programmed/updated (e.g., cold site) or operational control centers at corporate sister plants where operators can instantly log in as if they were located at the original location (e.g., hot site).

6.1.2 Is There a Contingency/Business Continuity Plan with Provider for Restoration?

The intent of this question is to identify and describe specific service level or special rate agreements that exist between the facility and the utility/service/product provider.

6.1.5 Restoration Time

The intent of this question is to determine the time needed for the facility to resume normal operations after the information technology service is restored. While in many cases the restoration time will be automatic/immediate, it is possible that a delay could occur due to the unique restoration requirements of certain processes or security verifications (i.e., lag time). The restoration time can vary based on the duration of the interruption. The answer to this question should be based on the Maximum Acceptable Outage (MAO) defined when considering the loss of information technology. If the MAO has not been defined, consider a maximum outage duration of 7 days: if the external source of information technology is lost during 7 days, what time will be needed for full resumption of core operations when information technology service is restored.

For purposes of this evaluation, recovery time is the time it takes to recover to a state of functionality whether at an alternative site or the present organization's site.

Alternative Site and Disaster Recovery	
Once the CCS is lost (without considering any redundant or alternative mode), what percentage of normal business functions are lost or degraded?	☐ 1–33% ☐ 34–66% ☐ 67–99% ☐ 100% (Offline)
Once the CCS is lost (without considering any redundant or alternative mode), within what time period will the business be severely impacted? Number of hours beyond which the effect of CCS loss is minimal.	_____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days)
Should your site become inoperable, do you have access to an alternative location?	☐ No ☐ Yes
Is there a contingency or business continuity agreement for recovery?	☐ No ☐ Yes If yes, explain: _____
If yes, how long does it take to recover the system at the alternative site? Number of hours beyond which activation of the alternative site is ineffective.	_____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days)
Does the organization employ measures to securely restore operation of cyber services after a disruption or organization incident?	☐ No ☐ Yes
Which of the following post-disaster measures does the organization have? *(Check all that apply.)*	☐ Alternative-site operations include cyber security measures consistent with those in place for ☐ Recovery/ reconstitution phases include cyber security measures consistent with those in place for ☐ Organization has Continuity of Operations Plans that include cyber security. ☐ Organization has Disaster Recovery Plans that include cyber security.

Alternative Site and Disaster Recovery				
	the original operational functions. ☐ Organization has Business Continuity Plans that include cyber security.	the original operational functions. ☐ Organization has cyber Contingency Plans that include cyber security.	☐ Organization has backups of data and software (e.g., firewall rules and control service configuration files) available such that services can be restored quickly to an equivalently secure state.	☐ Organization has no documented measures.
How often do you test your alternative-site procedures/capabilities?	☐ Never ☐ Every two years ☐ Annually ☐ More than once a year			
How do you test alternative-site procedures/capabilities?	☐ With a controlled live-fire incident chosen by an outside source ☐ With a controlled live-fire incident chosen by an inside source ☐ With a tabletop exercise ☐ Via document review			
Alternate Site and Disaster Recovery Briefing Notes: _____				
Alternate Site and Disaster Recovery Comments: _____				

7.0 Dependencies (LEVEL ONE)

Dependencies at rest – items such as storage (SAN, NAS)

Dependencies in motion – switches, networks, firewalls

Dependencies in process – mainframe & cluster

7.1 Dependencies – Data at Rest (LEVEL TWO)

Dependencies – Data at Rest	
Is data storage required for the CCS? ('No' means CCS is not dependent on data storage; 'No' is best answer.)	☐ No ☐ Yes
If the storage gear (SAN, NAS, etc.) becomes unavailable, within what time period will the CCS be severely impacted (i.e., lost connectivity, misconfiguration, device failure)? Number of hours beyond which the effect on the CCS is minimal.	_____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days)
Once the storage gear (SAN, NAS, etc.) has become unavailable (without considering any redundant or alternative mode), what percentage of normal cyber functions are lost or degraded?	☐ 1–33% ☐ 34–66% ☐ 67–99% ☐ 100% (Offline)
Does the organization have alternative or backup storage capabilities that can be used in case of loss of the primary storage?	☐ No ☐ Yes
Once the primary storage is restored, how long will it take before full resumption of operations? Number of hours beyond which resumption of operations is ineffective.	_____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Describe: _____

Data at Rest Dependencies Briefing Notes: _____
Data at Rest Dependencies Comments: _____

7.2 Dependencies – Data in Motion (LEVEL TWO)

Dependencies – Data in Motion	
Are external communications required for the organization's cyber operations? ('No' means that CCS is not dependent on external communications; 'No' is best answer.)	☐ No ☐ Yes If yes, who/what is the dependency on? ☐ Networking provider: _____ ☐ Telecom provider: _____ If yes, is the dependency provider required to notify the organization of an outage? ☐ No ☐ Yes If yes, do you monitor this dependency? ☐ No ☐ Yes
Are internal communications required for the organization's cyber operations?	☐ No ☐ Yes If yes, who/what is the dependency on? ☐ Networking provider: _____ ☐ Telecom provider: _____ If yes, is the dependency provider required to notify the organization of an outage? ☐ No ☐ Yes If yes, do you monitor this dependency? ☐ No ☐ Yes
If the communication services functionality (switches, network, firewalls, etc.) is lost completely, within what time period will the CCS be severely impacted? Number of hours beyond which the effect on the CCS is minimal.	_____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days)

Once the functionality of the communication services (switches, network, firewalls, etc.) is lost (without considering any redundant or alternative mode), what percentage of normal cyber functions are lost or degraded?	☐ 1–33% ☐ 34–66% ☐ 67–99% ☐ 100% (Offline)
Is there a contingency/business continuity plan with the provider for restoration?	☐ No ☐ Yes Explain: _____
Does the organization participate in the provider's priority plan for restoration?	☐ No ☐ Yes Explain: _____
If the primary mode of communication service is lost, is there a backup mode of communication?	☐ No ☐ Yes Explain: _____
Once the primary mode is restored, how long will it take before full resumption of operations? Number of hours beyond which resumption of operations is ineffective.	_____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Describe: _____
Data in Motion Dependencies Briefing Notes: _____	
Data in Motion Dependencies Comments: _____	

7.3 Dependencies – Data in Process (LEVEL TWO)

Dependencies – Data in Process	
Are data processing services (mainframes, server farms, cloud providers, etc.) required for the operation of the CCS? ('No' means that CCS is not dependent on data processing services; 'No' is best answer.)	☐ No ☐ Yes
If power to the processing service (mainframe, cluster, etc.) is lost completely, within what time period will the CCS be severely impacted? Number of hours beyond which the effect on the CCS is minimal.	_____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days)
Once the availability of the processing service (mainframe, cluster, etc.) is lost (without considering any redundant or alternative mode), what percentage of normal cyber functions are lost or degraded?	☐ 1-–33% ☐ 34–66% ☐ 67–99% ☐ 100% (Offline)
Is there a contingency/business continuity plan with the provider for restoration?	☐ No ☐ Yes Explain: _____
Once service is restored, how long will it take before full resumption of operations? Number of hours beyond which resumption of operations is ineffective.	_____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Describe: _____
Does the organization depend on external data service providers? ('No' is best answer.)	☐ No ☐ Yes If yes, who/what is the dependency on:

	☐ Data set: _____ ☐ Analytic capability: _____ If yes, Is the dependency provider required to notify the organization of an outage? ☐ No ☐ Yes If yes, do you monitor this dependency? ☐ No ☐ Yes
Data in Process Dependencies Briefing Notes: _____	
Data in Process Dependencies Comments: _____	

7.4 Dependencies – End Point Services (LEVEL TWO)

Dependencies – End Point Systems	
Are end-point systems (desktops, laptops, tablets, etc.) required for the operation of the CCS? ('No' means that CCS is not dependent on endpoint systems, 'No' is best answer.)	☐ No ☐ Yes
If the endpoint systems (desktops, laptops, tablets, etc.) are no longer available, within what time period would the CCS be severely impacted? Number of hours beyond which the effect on the CCS is minimal.	_____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days)
Once the endpoint systems (desktops, laptops, tablets, etc.) are no longer available (without considering any redundant or alternative mode), what percentage	☐ 1–33% ☐ 34–66% ☐ 67–99% ☐ 100% (Offline)

of normal cyber functions are lost or degraded?	
Is there a contingency/business continuity plan with the provider for restoration?	☐ No ☐ Yes *Explain*: _____
Does the organization participate in the provider's priority plan for restoration?	☐ No ☐ Yes *Explain*: _____
Once the primary service is restored, how long will it take before full resumption of operations? Number of hours beyond which resumption of operations is ineffective.	_____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Describe: _____
End Point Services Dependencies Briefing Notes: _____	
End Point Services Dependencies Comments: _____	