	CY - BASE
1.000	**IDENTIFY**
1.001	Does your agency have a cybersecurity program?
1.002	Does your agency have written and approved cybersecurity policy, plan, process, and supporting procedures?
1.003	Do your cybersecurity plans incorporate any of the following approaches/guidance?
	*National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity
	*NIST 800-171- Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
	*NIST 800-82 - Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection
	*NIST Special Publication 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations
	*ISO/IEC 27001 - Information Security Management
	*U.S. Department of Homeland Security, Transportation Systems Sector Cybersecurity Framework Implementation Guidance
	*Industry-specific methodologies (See APTA categories)
	*Other (if checked, elaborate)
1.004	Does your agency review, assess, and update as necessary all cybersecurity policies, plans, processes, and supporting procedures at least every 12 months, or when there is a significant organizational or technological change?
1.005	For critical cyber assets (i.e. "critical cyber asset" – a cyber asset that performs one or more operationally critical tasks), does your agency review, assess, and update as necessary all cybersecurity policies plans, processes, and supporting procedures at least every 12 months, or when there is a significant organizational change?
1.006	Does your agency evaluate and classify cyber assets using the following criteria?
	*Cyber Assets - Programmable electronic devices, including the hardware, software, and data in those devices?
	*Critical Cyber Asset – A cyber asset that performs one or more operationally critical tasks?
	*Cyber System - One or more critical cyber assets logically grouped by an agency to perform one or more operationally critical tasks?
1.007	Does your agency review and assess cyber asset classification as critical or noncritical at least every 12 months?
	*Cyber Assets - Programmable electronic devices, including the hardware, software, and data in those devices?
	*Critical Cyber Asset – A cyber asset that performs one or more operationally critical tasks?
	*Cyber System - One or more critical cyber assets logically grouped by an agency to perform one or more operationally critical tasks?
1.008	Does your organization have a cybersecurity risk assessment process?
1.009	Does your organization conduct cyber vulnerability assessments as described in your risk assessment process in the following environments?
	*OT environment?
	* IT environment?
1.010	Has your organization conducted a risk assessment to identify operational control(s) and communication/business enterprise assets and potential vulnerabilities at least every 12 months in the following environments?
	*OT environment?
	* IT environment?
1.011	Has your organization conducted a risk assessment to identify cyber assets and their vulnerabilities using the following criteria?
	* IT(devices that support communication, business enterprise)?

	* IT/OT (devices that support the operations and ICS environment)?
	*ICS (cyber systems for operations and management)?
	*Operational control(s) and communication/business enterprise IT assets and potential vulnerabilities?
1.012	Does the vulnerability management process address unmitigated/accepted vulnerabilities in the following environments?
	*OT environment?
	* IT environment?
1.013	Has your organization established a process to identify and evaluate vulnerabilities and compensating security controls?
1.014	Has a written cybersecurity incident response strategy been developed and integrated into the overall cybersecurity program?
1.015	For critical assets, has an inventory of the components of the operating system been developed, documented, and maintained for the following?
	*Current OT System?
	*Current IT System?
1.016	For critical cyber assets, is there a defined list of software programs authorized to execute in the operating system?
1.017	Does your agency have architecture and/or logic diagrams (i.e. components in a control system, Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs))?
1.018	Are methods in place to verify the accuracy of the architecture and/or logic diagrams (i.e. components in a control system, Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs)) and/or other documentation related to your OT system?
1.019	Has the agency implemented protocols to ensure that all facilities (e.g., data centers, server rooms, etc.) and equipment are properly secured to guard against internal or external cyber threats or attacks?
	*Current OT System?
	*Current IT System?
1.020	Are insider threats considered when vetting/assessing new hires and existing agency’s staff to include employees and contract personnel?
1.021	Are hardware/software components of a system evaluated and optimized to prevent vulnerabilities that can be exploited by a remote attacker?
1.022	If third-party service providers have access to the agency's system, are they properly vetted?
1.023	Does the agency have an established network security baseline for the following?
	*OT?
	*IT?
1.024	Has your agency taken actions to ensure their supply chain policies, procedures, and processes—include acquisition, receipt, warehouse, inventory control, and distribution—when acquiring vehicles, equipment, goods and services to ensure that cybersecurity risks are addressed?
1.025	Are IT and OT hardware, software and services addressed in the organization’s supply chain risk management program and policies?
1.026	Has your organization accurately and completely mapped the IT and OT supply chain including a list of companies that you procure assets, hardware, software and services from?
1.027	Has your organization identified an essential list of IT and OT components (e.g., hardware, software, services) for your business to operate?
1.028	Does your organization have written and approved program and policies regarding the procurement of IT and OT hardware and software (i.e. NIST standards compliant)?
1.029	Does your organization evaluate the security of IT and OT providers including security requirements and audits?
2.000	**PROTECT**

2.001	Does your agency have a designated and alternate cybersecurity representative and/or team responsible for the following?
	*OT?
	*IT?
2.002	Does the agency provide cybersecurity training?
	*Annually?
2.003	Does the agency ensure that recurring cybersecurity training reinforces security roles, responsibilities, and duties of employees at all levels to protect against and recognize cyber threats for the following?
	*OT?
	*IT?
2.004	For critical cyber assets, does your agency provide role-based security training on recognizing and reporting potential indicators of system compromise prior to granting access to critical cyber assets?
2.005	Are all personnel requiring access to the agency's cyber assets provided initial onboarding and subsequent annual cybersecurity awareness training?
2.006	Is there a cybersecurity awareness program for employees that includes practical exercises/testing for the following?
	*OT?
	*IT?
2.007	Has your agency developed and distributed cybersecurity policies, plans, processes, and supporting procedures to the appropriate personnel?
2.008	Has your agency established and documented policies and procedures for the following?
	*Access Control
	*Awareness and Training
	*Audit and Accountability
	*Configuration Management/Baseline security controls
	*Cyber Asset Management and Maintenance/Change Management
	*Cybersecurity Incident Response
	*Identification and Authentication
	*Information Protection
	*Insider Threat
	*Media Protection
	*Patch Management
	*Personnel Security
	*Physical Protection (related to cyber systems, cyber assets, communications)
	*Recovery (disaster, business continuity) plan(s)
	*Risk Assessment
	*Security Assessment
2.009	Has your agency developed and maintained a comprehensive set of network/system architecture diagrams or other documentation, including nodes, interfaces, remote and third-party connections, and information flows?
2.010	Does the agency have policies and processes in place to inventory operational control (OT) and enterprise (IT) assets, including hardware, software and applications?
2.011	Has your agency developed an operational framework to ensure coordination, communication, and accountability for information security on and between the control systems and enterprise networks?
2.012	Has your agency implemented the following measures?
	*Establish and enforce unique accounts for each individual user and administrator?
	*Establish and enforce access control policies for local and remote users?
	*Prohibit the sharing of these accounts?
	*Procedures and controls in place for approving and enforcing remote and third-party connections?

2.013	Are authentication methods and specific standards employed throughout your company’s cyber access control environment?
2.014	Where systems do not support unique user accounts, are appropriate compensating security controls (e.g., physical controls) implemented?
2.015	Does your agency ensure user accounts are modified, deleted, or de-activated expeditiously for personnel who no longer require access or are no longer employed by the organization?
2.016	Does your agency ensure appropriate segregation of duties is in place and, where this is not feasible, apply appropriate compensating security controls?
2.017	Does your agency change all default passwords for new software, hardware, etc., upon installation and, where this is not feasible (e.g., a control system with a hard-wired password), implement appropriate compensating security controls (e.g., administrative controls)?
2.018	For critical cyber assets, has your agency implemented the following measures?
	*Restrict user physical access to control systems and control networks by using appropriate controls?
	*Employ more stringent identity and access management practices (e.g., authenticators, permissions, password-construct, access control)?
	*Tiered administrative access based on need to access the different systems?
2.019	Does your agency monitor physical and remote user access to critical cyber assets?
2.020	Does your agency employ mechanisms (e.g., active directory) to support the management of accounts for critical cyber assets?
2.021	Has your agency established and implemented policies and procedures to ensure data protection measures are in place, including the following?
	*Identifying critical data and establishing classification of different types of data.
	*Establishing specific data handling procedures.
	*Establishing specific data disposal procedures.
2.022	If data protection measures are not in place, are compensating controls in place?
2.023	Are cyber assets segregated and protected from enterprise networks and the internet by use of physical separation, firewalls, and other protections (OT and IT – SCADA systems and Payment Systems etc.)?
2.024	Does the OT/IT system deny network traffic by default and allow only authorized network traffic?
2.025	Does the OT system monitor and manage communications at appropriate OT network boundaries?
2.026	Do OT system controls protect the integrity of electronically-communicated information? (e.g., preventing man in the middle)?
2.027	Does the OT system prevent traffic from being routed to the internet?
2.028	Does your agency regularly validate that technical controls comply with the organization's cybersecurity policies, plans, and procedures, and report results to senior management?
2.029	Has your agency implemented technical or procedural controls to restrict the use of cyber assets to only approved activities?
2.030	Does the agency prioritize protection for accounts with elevated privileges, remote access, and/or used on high value assets by using a multi-factor authentication approach for the identified high-value assets?
2.031	Does the agency maintain control via VPN or some other means as it relates to accessing the agencies cyber infrastructure via the use of personally owned devices, e.g. Android, iPhone, iPad, etc.?
2.032	Does the agency have a method for severing the connection/disconnecting access to personally owned devices when the employee has left the agency ?
3.000	**DETECT**
3.001	Does the agency have documented IT roles and responsibilities?
3.002	For critical cyber assets, does your agency employ mechanisms to detect unauthorized components?
3.003	For critical cyber assets, does your agency review network connections periodically, including remote access and third-party connections?
3.004	Has your agency implemented processes to respond to anomalous activity through the following?
	*Generating alerts and responding to them in a timely manner?

	*Logging cybersecurity events and reviewing these logs?
	*Are logs regularly analyzed and maintained for a minimum of 12 months?
3.005	Does your agency monitor for unauthorized access or the introduction of malicious code or communications?
3.006	Has your agency established technical or procedural controls for cyber intrusion monitoring and detection?
3.007	Does your agency perform regular testing of intrusion and malware detection processes and procedures (e.g., penetration testing)?
3.008	Does the agency take proactive measures to detect, contain, and remove malicious presence within the network?
3.009	Does the agency have mechanisms in place to analyze cyber anomalies for the following?
	*OT?
	*IT?
3.010	Does the agency have established documented incremental alert levels for cyber incidents?
3.011	Does the agency have mechanisms in place to ensure continuous monitoring of the following?
	*OT systems?
	*IT systems?
3.012	Does the agency audit and test its IT monitoring systems to verify effectiveness?
	*Independent (internal) review annually?
	*3rd party (external) review every 3 years?
3.013	Has your agency invested in cybersecurity assessment in the last 5 years?
	*Independent (internal) review in the last 5 years?
	*3rd party (external) review in the last 5 years
3.014	Does your agency employ Threat Hunting/Red Teaming to identify existing threats on the network?
4.000	**RESPOND**
4.001	Has your agency established policies and procedures for cybersecurity incident handling, analysis, and notifications (reporting/alerting), including assignments of specific roles/tasks to individuals and teams?
4.002	Has your agency established and maintained a cyber-incident response capability?
4.003	For critical cyber assets, has your agency established and maintained a process that supports 24/7 cyber-incident response?
4.004	Do your agency's response plans and procedures include mitigation measures to help prevent further impacts?
4.005	Does the organization have procedures in place for reporting incidents through the appropriate channels (i.e. local FBI and CISA cyber incident response office(s)) and also contacting TSA's Transportation Security Operations Center (TSOC) for actual or suspected cyber-attacks that could impact transportation operations?
5.000	**RECOVER**
5.001	Has your agency established a plan for the recovery and reconstitution of cyber assets within a time frame to align with the organization's safety and business continuity objectives?
5.002	Has the agency developed, separately or as part of another document, recovery plans in the event of a cybersecurity incident for the following?
	*IT(devices that support communication, business enterprise)?
	*IT/OT (devices that support the operations and ICS/SCADA environment)?
	*ICS/SCADA (cyber systems that are used to perform transit operations and management)?
5.003	Does your agency review its cyber recovery plan annually and update it as necessary?
5.004	For critical cyber assets, are cybersecurity incident response exercises conducted as follows?
	*Quarterly?
	*Semi-annually?
	*Annually?
5.005	Does the agency document lessons learned and incorporate them into cybersecurity planning and training?
5.006	Does the agency have documented procedures in place to coordinate restoration efforts with internal and external stakeholders (coordination centers, Internet Service Providers, victims, vendors, etc.)?

5.007	Does the agency conduct System Recovery Plan exercises at least every 12 months to ensure the restoration of data as part of their comprehensive disaster recovery strategy?

Paperwork Reduction Act Burden Statement: This is a voluntary collection of information. TSA estimates that the total average burden per response associated with this collection is approximately 7.8 hours. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a valid OMB control number. The control number assigned to this collection is OMB 1652-0062, which expires on 05/31/2024. Send comments regarding this burden estimate or collection to TSA-11, Attention: PRA 1652-0062 BASE, 6595 Springfield Center Drive, Springfield, VA 20598-6011.