Proposed Cybersecurity Questions - MT BASE (Cybersecurity Annex)		NIST Category
Section	Description	
1.100	**Cybersecurity Annex**	
1.100	**IDENTIFY**	
1.101	Does your agency have a cybersecurity program?	Asset Management
1.102	Does your agency have written and approved cybersecurity policy, plan, process, and supporting procedures?	Asset Management
1.103	Do your cybersecurity plans incorporate any of the following approaches/guidance?	Asset Management
	*National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity	Asset Management
	*NIST 800-171 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	Asset Management
	*NIST 800-82 - Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection	Asset Management
	*NIST Special Publication 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations	Asset Management
	*ISO/IEC 27001 - Information Security Management	Asset Management
	*U.S. Department of Homeland Security, Transportation Systems Sector Cybersecurity Framework Implementation Guidance	Asset Management
	*Industry-specific methodologies (See APTA categories)	Asset Management
	*Other (if checked, elaborate)	Asset Management
1.104	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?	Governance
1.105	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?	Governance
1.106	Does your agency evaluate and classify cyber assets using the following criteria?	Business Environment
	*Cyber Assets - Programmable electronic devices, including the hardware, software, and data in those devices?	Business Environment
	*Critical Cyber Asset – A cyber asset that performs one or more operationally critical tasks?	Business Environment
	*Cyber System - One or more critical cyber assets logically grouped by an agency to perform one or more operationally critical tasks?	Business Environment
1.107	Does your agency review and assess cyber asset classification as critical or noncritical at least every 12 months?	Business Environment
	*Cyber Assets - Programmable electronic devices, including the hardware, software, and data in those devices?	Business Environment
	*Critical Cyber Asset – A cyber asset that performs one or more operationally critical tasks?	Business Environment
	*Cyber System - One or more critical cyber assets logically grouped by an agency to perform one or more operationally critical tasks?	Business Environment

1.108	Does your organization have a cybersecurity risk assessment process?	Business Environment
1.109	Does your organization conduct cyber vulnerability assessments as described in your risk assessment process in the following environments?	Business Environment
	*OT environment?	Business Environment
	* IT environment?	Business Environment
1.110	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?	Risk Assessment
	*OT environment?	Risk Assessment
	* IT environment?	Risk Assessment
1.111	Has your organization conducted a risk assessment to identify cyber assets and their vulnerabilities using the following criteria?	Risk Assessment
	* IT(devices that support communication, business enterprise)?	Risk Assessment
	* IT/OT (devices that support the operations and ICS environment)?	Risk Assessment
	*ICS (cyber systems for operations and management)?	Risk Assessment
	*Operational control(s) and communication/business enterprise IT assets and potential vulnerabilities?	Risk Assessment
1.112	Does the vulnerability management process address unmitigated/accepted vulnerabilities in the following environments?	Risk Assessment
	*OT environment?	Risk Assessment
	* IT environment?	Risk Assessment
1.113	Has your organization established a process to identify and evaluate vulnerabilities and compensating security controls?	Risk Assessment
1.114	Has a written cybersecurity incident response strategy been developed and integrated into the overall cybersecurity program?	Risk Management Strategy
1.115	For critical assets, has an inventory of the components of the operating system been developed, documented, and maintained for the following?	Risk Assessment
	*Current OT System?	Risk Assessment
	*Current IT System?	Risk Assessment
1.116	For critical cyber assets, is there a defined list of software programs authorized to execute in the operating system?	Risk Assessment
1.117	Does your agency have architecture and/or logic diagrams (i.e. components in a control system, Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs))?	Business Environment
1.118	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?	Business Environment
1.119	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?	Supply Chain Management

	*Current OT System?	Risk Assessment
	*Current IT System?	Risk Assessment
1.120	Are insider threats considered when vetting/assessing new hires and existing agency's staff to include employees and contract personnel?	Asset Management
1.121	Are hardware/software components of a system evaluated and optimized to prevent vulnerabilities that can be exploited by a remote attacker?	Asset Management
1.122	If third-party service providers have access to the agency's system, are they properly vetted?	Asset Management
1.123	Does the agency have an established network security baseline for the following?	Asset Management
	*OT?	Asset Management
	*IT?	Asset Management
1.124	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?	Supply Chain Management
1.125	Are IT and OT hardware, software and services addressed in the organization's supply chain risk management program and policies?	Supply Chain Management
1.126	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?	Supply Chain Management
1.127	Has your organization identified an essential list of IT and OT components (e.g., hardware, software, services) for your business to operate?	Supply Chain Management
1.128	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)?	Supply Chain Management
1.129	Does your organization evaluate the security of IT and OT providers including security requirements and audits?	Supply Chain Management
1.200	**PROTECT**	
1.201	Does your agency have a designated and alternate cybersecurity representative and/or team responsible for the following?	Identity Management & Access Control
	*OT?	Identity Management & Access Control
	*IT?	Identity Management & Access Control
1.202	Does the agency provide cybersecurity training?	Awareness and Training
	*Annually?	Awareness and Training
1.203	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?	Awareness and Training

	*OT?	Awareness and Training
	*IT?	Awareness and Training
1.204	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?	Awareness and Training
1.205	Are all personnel requiring access to the agency's cyber assets provided initial onboarding and subsequent annual cybersecurity awareness training?	Awareness and Training
1.206	Is there a cybersecurity awareness program for employees that includes practical exercises/testing for the following?	Awareness and Training
	*OT?	Awareness and Training
	*IT?	Awareness and Training
1.207	Has your agency developed and distributed cybersecurity policies, plans, processes, and supporting procedures to the appropriate personnel?	Awareness and Training
1.208	Has your agency established and documented policies and procedures for the following?	Data Security
	*Access Control	Data Security
	*Awareness and Training	Data Security
	*Audit and Accountability	Data Security
	*Configuration Management/Baseline security controls	Data Security
	*Cyber Asset Management and Maintenance/Change Management	Data Security
	*Cybersecurity Incident Response	Data Security
	*Identification and Authentication	Data Security
	*Information Protection	Data Security
	*Insider Threat	Data Security
	*Media Protection	Data Security
	*Patch Management	Data Security
	*Personnel Security	Data Security
	*Physical Protection (related to cyber systems, cyber assets, communications)	Data Security
	*Recovery (disaster, business continuity) plan(s)	Data Security
	*Risk Assessment	Data Security
	*Security Assessment	Data Security
1.209	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?	Data Security
1.210	Does the agency have policies and processes in place to inventory operational control (OT) and enterprise (IT) assets, including hardware, software and applications?	Data Security
1.211	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?	Data Security

1.212	Has your agency implemented the following measures?	Data Security
	*Establish and enforce unique accounts for each individual user and administrator?	Data Security
	*Establish and enforce access control policies for local and remote users?	Data Security
	*Prohibit the sharing of these accounts?	Data Security
	*Procedures and controls in place for approving and enforcing remote and third-party connections?	Data Security
1.213	Are authentication methods and specific standards employed throughout your company's cyber access control environment?	Data Security
1.214	Where systems do not support unique user accounts, are appropriate compensating security controls (e.g., physical controls) implemented?	Data Security
1.215	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?	Data Security
1.216	Does your agency ensure appropriate segregation of duties is in place and, where this is not feasible, apply appropriate compensating security controls?	Data Security
1.217	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)?	Data Security
1.218	For critical cyber assets, has your agency implemented the following measures?	Data Security
	*Restrict user physical access to control systems and control networks by using appropriate controls?	Data Security
	*Employ more stringent identity and access management practices (e.g., authenticators, permissions, password-construct, access control)?	Data Security
	*Tiered administrative access based on need to access the different systems?	Data Security
1.219	Does your agency monitor physical and remote user access to critical cyber assets?	Information Protection Processes & Procedures
1.220	Does your agency employ mechanisms (e.g., active directory) to support the management of accounts for critical cyber assets?	Information Protection Processes & Procedures
1.221	Has your agency established and implemented policies and procedures to ensure data protection measures are in place, including the following?	Information Protection Processes & Procedures
	*Identifying critical data and establishing classification of different types of data.	Information Protection Processes & Procedures
	*Establishing specific data handling procedures.	Information Protection Processes & Procedures
	*Establishing specific data disposal procedures.	Information Protection Processes & Procedures

1.222	If data protection measures are not in place, are compensating controls in place?	Information Protection Processes & Procedures
1.223	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.)?	Information Protection Processes & Procedures
1.224	Does the OT/IT system deny network traffic by default and allow only authorized network traffic?	Information Protection Processes & Procedures
1.225	Does the OT system monitor and manage communications at appropriate OT network boundaries?	Information Protection Processes & Procedures
1.226	Do OT system controls protect the integrity of electronically-communicated information? (e.g., preventing man in the middle)?	Information Protection Processes & Procedures
1.227	Does the OT system prevent traffic from being routed to the internet?	Information Protection Processes & Procedures
1.228	Does your agency regularly validate that technical controls comply with the organization's cybersecurity policies, plans, and procedures, and report results to senior management?	Information Protection Processes & Procedures
1.229	Has your agency implemented technical or procedural controls to restrict the use of cyber assets to only approved activities?	Information Protection Processes & Procedures
1.230	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?	Information Protection Processes & Procedures
1.231	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.?	Protective Technology
1.232	Does the agency have a method for severing the connection/disconnecting access to personally owned devices when the employee has left the agency ?	Protective Technology
1.300	**DETECT**	
1.301	Does the agency have documented IT roles and responsibilities?	Anomalies and Events
1.302	For critical cyber assets, does your agency employ mechanisms to detect unauthorized components?	Anomalies and Events
1.303	For critical cyber assets, does your agency review network connections periodically, including remote access and third-party connections?	Anomalies and Events
1.304	Has your agency implemented processes to respond to anomalous activity through the following?	Anomalies and Events
	*Generating alerts and responding to them in a timely manner?	Anomalies and Events

	*Logging cybersecurity events and reviewing these logs?	Anomalies and Events
	*Are logs regularly analyzed and maintained for a minimum of 12 months?	Anomalies and Events
1.305	Does your agency monitor for unauthorized access or the introduction of malicious code or communications?	Security Continuous Monitoring
1.306	Has your agency established technical or procedural controls for cyber intrusion monitoring and detection?	Security Continuous Monitoring
1.307	Does your agency perform regular testing of intrusion and malware detection processes and procedures (e.g., penetration testing)?	Detection Processes
1.308	Does the agency take proactive measures to detect, contain, and remove malicious presence within the network?	Detection Processes
1.309	Does the agency have mechanisms in place to analyze cyber anomalies for the following?	Anomalies and Events
	*OT?	Anomalies and Events
	*IT?	Anomalies and Events
1.310	Does the agency have established documented incremental alert levels for cyber incidents?	Anomalies and Events
1.311	Does the agency have mechanisms in place to ensure continuous monitoring of the following?	Security Continuous Monitoring
	*OT systems?	Security Continuous Monitoring
	*IT systems?	Security Continuous Monitoring
1.312	Does the agency audit and test its IT monitoring systems to verify effectiveness?	Security Continuous Monitoring
	*Independent (internal) review annually?	Security Continuous Monitoring
	*3rd party (external) review every 3 years?	Security Continuous Monitoring
1.313	Has your agency invested in cybersecurity assessment in the last 5 years?	Detection Processes
	*Independent (internal) review in the last 5 years?	Detection Processes
	*3rd party (external) review in the last 5 years	Detection Processes
1.314	Does your agency employ Threat Hunting/Red Teaming to identify existing threats on the network?	Detection Processes
1.400	**RESPOND**	
1.401	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?	Response Planning
1.402	Has your agency established and maintained a cyber-incident response capability?	Response Planning
1.403	For critical cyber assets, has your agency established and maintained a process that supports 24/7 cyber-incident response?	Response Planning

1.404	Do your agency's response plans and procedures include mitigation measures to help prevent further impacts?	Response Planning
1.405	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?	Communications
1.500	**RECOVER**	
1.501	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?	Recovery Planning
1.502	Has the agency developed, separately or as part of another document, recovery plans in the event of a cybersecurity incident for the following?	Recovery Planning
	*IT(devices that support communication, business enterprise)?	Recovery Planning
	*IT/OT (devices that support the operations and ICS/SCADA environment)?	Recovery Planning
	*ICS/SCADA (cyber systems that are used to perform transit operations and management)?	Recovery Planning
1.503	Does your agency review its cyber recovery plan annually and update it as necessary?	Recovery Planning
1.504	For critical cyber assets, are cybersecurity incident response exercises conducted as follows?	Recovery Planning
	*Quarterly?	Recovery Planning
	*Semi-annually?	Recovery Planning
	*Annually?	Recovery Planning
1.505	Does the agency document lessons learned and incorporate them into cybersecurity planning and training?	Improvements
1.506	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.)?	Communications
1.507	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?	Improvements

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 6 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.