	Proposed Cybersecurity SAI Questions - MT BASE	NIST Category
Section	**Description**	
11.000	**Developing a Comprehensive Cybersecurity Strategy (In accordance with NIST Framework)**	
11.100	**IDENTIFY**	
11.101	Does your agency have a cybersecurity program?	Asset Management
11.102	Does your agency have written and approved cybersecurity policy, plan, process, and supporting procedures?	Asset Management
11.103	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
11.104	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
11.105	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
11.106	Has a written cybersecurity incident response strategy been developed and integrated into the overall cybersecurity program?	Risk Management Strategy
11.107	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
11.200	**PROTECT**	
11.201	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
11.202	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
11.203	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
11.204	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
11.300	**DETECT**	
11.301	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
11.302	Does your agency monitor for unauthorized access or the introduction of malicious code or communications?	Security Continuous Monitoring

11.303	Has your agency established technical or procedural controls for cyber intrusion monitoring and detection?	Security Continuous Monitoring
11.400	**RESPOND**	
11.401	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
11.402	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
11.500	**RECOVER**	
11.501	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
11.502	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
11.503	Does your agency review its cyber recovery plan annually and update it as necessary?	Recovery Planning
11.504	Does the agency document lessons learned and incorporate them into cybersecurity planning and training?	Improvements
11.505	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

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.