Section	
	MANAGEMENT AND ACCOUNTABILITY
1.000	**Establish Written System Security Plans (SSPs)**
1.101	Does the transit agency have a System Security Plan (SSP) addressing personnel, facility, and vehicle security, and threat, vulnerability management?
1.102	Does the SSP identify goals and objectives for the security program? Are the goals and objectives for the security program actively monitored?
1.103	Has the SSP been reviewed, approved and adopted by top management, such as the agency's chief executive.
1.104	Does the SSP address protection and response for critical systems? (e.g., facilities, stations, terminals, offices building, underwater tunnels, underground stations/ tunnels and other critical systems)
1.105	Does the SSP establish procedures for the management of security incidents by the operations control center (or dispatch center) or other means?
1.106	Does the SSP contain or reference other documents establishing plans, procedures, or protocols for responding to security events with external agencies (e.g., law enforcement, local emergency management agency, fire departments, etc.)?
1.107	Does the SSP contain or reference documents for responding to active assailant events and partnered with local law enforcement/ first responders in the development of active assailant procedures or protocols?
1.108	Does the SSP contain or reference other documents that establish protocols addressing specific threats from Chemical, Biological, Radiological, Nuclear, Energetic (CBRNE)?
1.109	Are visible, random security measures based on employee type, integrated into security plans to introduce unpredictability in security activities for deterrent effect?
1.110	Does the SSP include provisions requiring that security be addressed in extensions, major projects, new vehicles and equipment procurement and other capital projects?
1.111	Does the SSP include or reference other documents adopting Crime Prevention Through Environmental Design (CPTED) principles as part of the agency's engineering practices?
1.112	Does the SSP require an annual review? When was the last time it was reviewed and is there documentation?
1.113	Does the transit agency produce periodic reports reviewing its progress in meeting its SSP goals and objectives?
1.114	Does the SSP contain or reference other documents to provide for Continuity of Operations (COOP) while responding to emergency events?
1.115	Does the agency have a written Business Recovery Plan to guide restoration of facilities and services following an emergency event?
1.116	Does the agency have a back-up operations control center capability?
2.000	**Define Roles and Responsibilities for Security Management**
2.101	Does the SSP establish and assign responsibility for implementation of the security program to a Senior Manager who is a "direct report" to the agency's Chief Executive Officer?
2.102	Has the agency established documented lines of delegated authority and lines of succession of security responsibilities?
2.103	Does the SSP or other documents establish roles and responsibilities for security and/or law enforcement personnel based on title and/or position?
2.104	Does the SSP or other documents establish security-related roles and responsibilities for non-security personnel based on title and/or position? (i.e., operators, conductors, maintenance workers and station attendants)
2.105	Do senior staff and middle management conduct security meetings to review recommendations for changes to plans and processes?
2.106	Does a Security Review Committee (or other designated group) regularly review security incident reports, trends, and program audit findings?
2.107	Are informational briefings with appropriate personnel held whenever security protocols, threat levels, or protective measures are updated or as security conditions warrant?
2.108	Have reference guides or other written instructions or procedures, appropriate to job function, been distributed to transit employees to implement the requirements of the SSP?

2.109	Has the agency appointed a Primary and Alternate Security Coordinator available 24-hr for intelligence and security-related contact with TSA and are the names and contact information of those coordinators on file with TSA Policy, Plans and Engagement correct?
2.110	Does the agency maintain a record of security related incidents that are reported within the agency?
3.000	**Ensure that operations and maintenance supervisors, forepersons and managers are held accountable for security issues under their control**
3.101	How frequently do managers and supervisors provide information to front-line personnel where security and emergency response issues are the primary focus?
3.102	How frequently are supervisor, manager, and/or foreperson security review and coordination briefings held?
3.103	Does the agency have a program that actively utilizes a formal process for confirming personnel have a measurable working knowledge of security protocols? (i.e. internal audits, challenge procedures, qualification testing)
3.104	Does the agency have a written policy requiring managers and/or supervisors to debrief front-line employees regarding their involvement in or management of any security incidents?
4.000	**Coordinate Security and Emergency Management Plan(s) with local and regional agencies**
4.101	Have Mutual Aid agreements been established between the transit agency and entities in the area that would be called upon to supplement the agency's resources in the event of an emergency event?
4.102	Does the agency participate in a regional Emergency Management Working Group or similar regional coordinating body for emergency preparedness and response?
4.103	Have regional incident management protocols been shared with the agency and incorporated into the agency's SSP?
4.104	Have agency resources been appropriately identified and provided to the regional EMA?
4.105	Does the agency have a designated point-of-contact or liaison from the local/regional Emergency Operations Center (EOC) or a representative to the local/regional EOC, should it be activated??
4.106	Has the agency developed internal incident management protocols that comply with the National Response Plan and the National Incident Management System (NIMS)?
4.107	Have the agency's emergency response protocols been shared with the EMA and appropriate first responder agencies?
4.108	Has the transit system tested its communications systems for interoperability with appropriate emergency response agencies?
4.109	If the agency's communications systems are NOT inter-operable with appropriate emergency response agencies, have alternate communication protocols been established? Describe the alternate communication protocols in the justification.
	SECURITY AND RESPONSE TRAINING
5.000	**Establish and Maintain a Security Training Program**
5.101	Is security training for new employees and annual refresher training provided to all employees regardless of position or job function from senior management to frontline employees, in a formal manner?
5.102	Is ongoing advanced security training focusing on job function provided at least annually?
5.103	Is active assailant training (run/fight/hide, Lockdown procedures or similar) provided to new and existing employees annually regardless of position or job function?
5.104	Is security training for new employees and annual refresher training regarding security incident response provided to all employees regardless of position or job function, from senior management to frontline employees, in a formal manner?
5.105	Do agency employees receive general training on Incident Command System (ICS) procedures in accordance with National Incident Management System (NIMS) appropriate to their position from senior management staff, and supervisors, to frontline employees? (Describe the frequency of training)
5.106	Has the agency developed and implemented security incident response protocols, and is annual refresher training provided to all employees regardless of position or job function from senior management, supervisors, to front line employees.

5.107	Has the transit system implemented an annual training program for personnel regarding response to terrorism, including CBRNE to all employees regardless of position or job function, from senior management to frontline employees, in a formal manner? If so, summarize the relevant programs in the justification?
5.108	Do law enforcement/security department personnel, security managers at the agency receive specialized training in counter-terrorism annually? Summarize program in the justification.
5.109	Do law enforcement/security department personnel at the agency receive specialized training supporting their security incident management? Summarize program in the justification.
5.110	Does the agency have an established program to track and maintain training records on all employees for all security-related courses (including initial, annual, periodic and other).
5.111	Does the agency have a program to regularly review and update security incident response training materials?
5.112	Are all appropriate personnel notified via briefings, email, voicemail, or signage of changes in threat condition, protective measures or the employee watch programs?
5.113	Do the agency's security awareness incident response training programs cover response and recovery operations in critical facilities and infrastructure? If so, summarize relevant provisions of program in the justification.
5.114	Has the agency provided training to regional first responders to enable them to operate in critical facilities and infrastructure?
5.115	Has the agency provided local law enforcement/first responders opportunities to familiarize themselves with agency’s system for response to security emergencies? (e.g. Active Assailant, etc.)
5.116	Does training of transit system law enforcement and/or security personnel integrate the concept and employment of visible, random security measures?
5.117	Has the agency implemented a program to train or orient first responders and other potential supporting assets (e.g., TSA regional personnel for VIPR exercises) on their system vehicle familiarization?
	HOMELAND SECURITY ADVISORY SYSTEM (HSAS)
6.000	**Establish plans and protocols to respond to the National Terrorism Advisory System (NTAS) alert system**
6.101	Does the SSP contain or reference other documents identifying incremental actions (imminent or elevated) to be implemented for a NTAS threat?
6.102	Does the agency have actionable operational response protocols for the specific threat scenarios from NTAS?
6.103	Has the agency provided annual training and/or instruction focused on job function regarding the incremental activities to be performed by employees?
	PUBLIC AWARENESS
7.000	**Implement and reinforce a Public Security and Emergency Awareness program**
7.101	Has the transit agency developed and implemented a public security awareness program?
7.102	Does the agency provide active public outreach for security awareness messages (e.g., “If You See Something, Say Something”, message boards, brochures, posters, fliers, etc.)?
7.103	Are the announcements for the public awareness program updated as needed, e.g., new leadership, or NTAS changes, etc.?
7.104	Are general security awareness messages included in public announcement messages at stations and on board vehicles?
7.105	Are passengers urged to report unattended property, suspicious behavior, and security concerns to uniformed crew members, law enforcement or security personnel, and/or a contact telephone number? If so, summarize the type of materials used and content in the justification.
7.106	Does the agency have an appropriate mechanism in place for passengers to communicate a security concern? (e.g., 1-800 number, smart phone applications, social media, etc.)
7.107	Does the agency issue public service announcements or press releases to social media regarding security protocols? (e.g. Twitter/ Facebook/etc., QRC codes, or Apps for smart phones)
7.108	Does the agency issue public service announcements or press releases to local media regarding security or emergency protocols? (e.g. newspaper, radio and/or television)

7.109	Do public awareness materials and/or messages inform passengers on the means to evacuate from transit vehicles and facilities, to include disabled or challenged individuals?
7.110	Does the agency track and monitor security related customer complaints, observations, activites reported by passengers?
	RISK MANAGEMENT
8.000	**Establish and use a risk management process**
8.101	Does the agency have its own risk assessment process, approved by its management, for managing threats and vulnerabilities? If so, summarize the process in the justification.
8.102	Has the agency identified facilities and systems it considers to be its critical assets?
8.103	Has the agency had an internal or external vulnerability assessment on its critical assets within the past 3 years? Specify the dates of the most recent assessments and the entity(ies) that conducted the assessment(s).
8.104	Has the agency had an internal or external Risk Assessment, analyzing threat, vulnerability, and consequence for critical assets and infrastructure, and systems within the past 3 years? Have management and staff responsible for the risk assessment process been formally trained to manage the process?
8.105	Has the system implemented procedures to limit and monitor access to underground and underwater tunnels? If so, summarize procedures in the justification.
8.106	Are security investments prioritized using information developed in the risk assessment process?
8.107	Upon request, has TSA been provided access to the agency's vulnerability assessments, Security Plan and related documents?
	ESTABLISH A RISK ASSESSMENT AND INFORMATION SHARING PROCESS
9.000	**Establish and use an information sharing process for threat and intelligence information.**
9.101	Does the agency have a formalized process and procedures for reporting and exchange of threat and intelligence information with Federal, State, and/or local law enforcement agencies?
9.102	Does the agency report threat and intelligence information directly to FBI Joint Terrorism Task Force (JTTF) or other regional anti-terrorism task force?
9.103	Does the agency have policies requiring employees to report (internal or external) suspicious activity to their supervisor or management?
9.104	Does the system have a protocol to report threats or significant security concerns to appropriate law enforcement authorities, and TSA's Transportation Security Operations Center (TSOC)?
9.105	Does the agency routinely receive threat and intelligence information directly from any Federal government agency, State Homeland Security Office, Regional or State Intelligence Fusion Center, PT-ISAC, or other transit agencies? If so, describe frequency.
	DRILLS AND EXERCISES
10.000	**Conduct Tabletop and Functional Drills**
10.101	Does the agency have a documented process to develop an approved, coordinated schedule for all security management program activities, including local/regional security planning and participation in exercises and drills?
10.102	Does the agency's or SSP describe or reference how the agency performs its security planning responsibilities and requirements regarding security incident drills and exercises?
10.103	Does the agency evaluate its security preparedness by using annual field exercises, tabletop exercises, and/or drills? If so, please summarize the exercise events held in the past year.
10.104	Does the agency's Security Preparedness Plan (SPP) or SSP document include a requirement for annual field exercises, tabletops and drills (e.g., I-STEP, EXIS, Cyber 5N5, etc.)
10.105	Does the agency's SPP or SSP describe or reference how the agency documents the results of its security preparedness evaluations? (i.e., briefings, after action reports and implementation of findings)
10.106	Does the agency's SPP or a related document describe or reference its security training program, response protocols and procedures?
10.107	Does the agency participate as an active player in full-scale, regional exercises, at least annually?
10.108	In the last 12 months, has the agency conducted drills or exercises specifically focus on active assailant scenarios with its employees?

10.109	In the last 12 months, has the agency conducted and/or participated in a drill, tabletop exercise, and/or field exercise including scenarios involving CBRNE with other transit agencies and first responders (e.g., NTAS scenarios)?
10.110	In the last year, has the agency reviewed results and prepared after-action reports to assess performance and develop lessons learned for all drills, tabletop, and/or field exercises.
10.111	In the last 12 months, has the agency updated plans, protocols and processes to incorporate after-action report recommendations/findings or corrective actions? If so, summarize the actions taken in the justification.
10.112	Has the agency established a system for objectively measuring and assessing its performance during security exercises and to measure improvements?
10.113	Does the system conduct drills and exercises of its security response plans to test capabilities of employees and first responders to operate effectively throughout the agencies system? (i.e., facilities, stations, office buildings, terminals, underwater/ underground infrastructure and other critical systems)
10.114	Does the transit system integrate local and regional first responders in drills, tabletop exercises, and/or field exercises? If so, summarize each joint event and state when it took place.
11.000	**DEVELOPING A COMPREHENSIVE CYBERSECURITY STRATEGY**
11.100	**Developing a Comprehensive Cybersecurity Strategy - Identify**
11.101	Does your agency have a cybersecurity program?
11.102	Does your agency have written and approved cybersecurity policy, plan, process, and supporting procedures?
11.103.00	Do your cybersecurity plans incorporate any of the following approaches/guidance? (DO NOT ask those entities covered by SD 1582-21-01 / 1582-21-01A)
11.103.01	National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity
11.103.02	NIST 800-171 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
11.103.03	NIST 800-82 - Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection
11.103.04	NIST Special Publication 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations
11.103.05	ISO/IEC 27001 - Information Security Management
11.103.06	U.S. Department of Homeland Security Transportation Systems Sector Cybersecurity Framework Implementation Guidance
11.103.07	Industry-specific methodologies (See APTA categories)
11.103.08	Other (if checked elaborate)
11.103.09	None of the above
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? (DO NOT ask those entities covered by SD 1582-21-01 / 1582-21-01A)
11.105.00	Does your organization conduct cyber vulnerability assessments as described in your risk assessment process in the following environments? (DO NOT ask those entities covered by SD 1582-21-01 / 1582-21-01A)
11.105.01	OT environment?
11.105.02	IT environment?
11.105.03	None of the above
11.106	Has a written cybersecurity incident response strategy been developed and integrated into the overall cybersecurity program?
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?
11.200	**Developing a Comprehensive Cybersecurity Strategy - Protect**
11.201.00	Does your agency have a designated and alternate cybersecurity representative and/or team responsible for the following?
11.201.01	OT environment?
11.201.02	IT environment?

11.201.03	None of the above
11.202.00	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?
11.202.01	OT environment?
11.202.02	IT environment?
11.202.03	None of the above
11.203.00	Has your agency established and documented policies and procedures for the following? (DO NOT ask those entities covered by SD 1582-21-01 / 1582-21-01A)
11.203.01	Access Control
11.203.02	Awareness and Training
11.203.03	Audit and Accountability
11.203.04	Configuration Management/Baseline security controls
11.203.05	Cyber Asset Management and Maintenance/Change Management
11.203.06	Cybersecurity Incident Response
11.203.07	Identification and Authentication
11.203.08	Information Protection
11.203.09	Insider Threat
11.203.10	Media Protection
11.203.11	Patch Management
11.203.12	Personnel Security
11.203.13	Physical Protection (related to cyber systems cyber assets communications)
11.203.14	Recovery (disaster business continuity) plan(s)
11.203.15	Risk Assessment
11.203.16	Security Assessment
11.203.17	Note of the above
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?
11.300	**Developing a Comprehensive Cybersecurity Strategy - Detect**
11.301.00	Has your agency implemented processes to respond to anomalous activity through the following? (DO NOT ask those entities covered by SD 1582-21-01 / 1582-21-01A)
11.301.01	Generating alerts and responding to them in a timely manner?
11.301.02	Logging cybersecurity events and reviewing these logs?
11.301.03	Are logs regularly analyzed and maintained for a minimum of 12 months?
11.301.04	None of the above
11.302	Does your agency monitor for unauthorized access or the introduction of malicious code or communications? (DO NOT ask those entities covered by SD 1582-21-01 / 1582-21-01A)
11.304	Has your agency established technical or procedural controls for cyber intrusion monitoring and detection? (DO NOT ask those entities covered by SD 1582-21-01 / 1582-21-01A)
11.400	**Developing a Comprehensive Cybersecurity Strategy - 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? (DO NOT ask those entities covered by SD 1582-21-01 / 1582-21-01A)
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? (DO NOT ask those entities covered by SD 1582-21-01 / 1582-21-01A)
11.500	**Developing a Comprehensive Cybersecurity Strategy - 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? (DO NOT ask those entities covered by SD 1582-21-01 / 1582-21-01A)
11.502.00	Has the agency developed, separately or as part of another document, recovery plans in the event of a cybersecurity incident for the following?

11.502.01	IT(devices that support communication business enterprise)?
11.502.02	1IT/OT (devices that support the operations and ICS/SCADA environment)?
11.502.03	ICS/SCADA (cyber systems that are used to perform transit operations and management)?
11.502.04	None of the above
11.503	Does your agency review its cyber recovery plan annually and update it as necessary? (DO NOT ask those entities covered by SD 1582-21-01 / 1582-21-01A)
11.504	Does the agency document lessons learned and incorporate them into cybersecurity planning and training?
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.)? (DO NOT ask those entities covered by SD 1582-21-01 / 1582-21-01A)
	FACILITY SECURITY AND ACCESS CONTROLS
12.000	**Control Access to Critical Facilities with ID badges for all visitors, employees and contractors**
12.101	Have assets and facilities requiring restricted access been identified?
12.102	Are ID badges or other measures employed to restrict access to facilities not open to the public?
12.103	Has the transit agency developed and implemented procedures to monitor, update and document access control (e.g. card key, ID badges, keys, safe combinations, etc.)?
12.104	Does the agency have documented procedures for issuing ID badges to visitors and contractors?
12.105	Does the agency have a documented policy that requires visitors to be escorted when accessing non-public areas.
12.106	Is CCTV equipment installed in transit agency facilities?
12.107	Is CCTV equipment protecting critical assets interfaced with an access control system?
12.108	Is CCTV equipment installed on transit vehicles?
12.109	Are Crime Prevention through Environmental Design (CPTED) and technology (e.g., CCTV, access control, intrusion detection, bollards, etc.) incorporated into design criteria for all new and/or existing capital projects?
12.110	Does the agency use fencing, barriers, and/or intrusion detection to protect against unauthorized entry into stations, facilities, and other identified critical assets?
12.111	Has the system implemented protective measures to secure high risk/high consequence assets and critical systems? (i.e., CCTV, intrusion detection systems, smart camera technology, fencing, enhanced lighting, access control, LE patrols, K-9s, protection of ventilation systems)
12.112	Does the transit agency monitor a network of security, fire, duress, intrusion, utility and internal 911 alarm systems?
12.113	Does the agency provide a method for passengers and visitors to report security and safety concerns from within the agency's system?
12.114	Does the transit agency administer an automated employee access control system and perform corrective analysis of security breaches?
12.115	Does the agency have policies and procedures for screening of mail and/or outside deliveries?
12.116	Have locks, bullet resistant materials and anti-fragmentation materials been installed/used at critical locations?
12.117	Is directional signage with adequate lighting provided in a consistent manner throughout their system, both to provide orientation and to support emergency evacuation?
12.118	Are gates and locks used on all facility doors to prevent unauthorized access during operating hours?
12.119	Are keys controlled through an established program that is documented?
12.120	Are gates and locks used to close down system facilities after operating hours?
12.121	Do transit vehicles have radios, silent alarms, and/or passenger communication systems?
12.122	Does the transit agency use graffiti-resistant/etch-resistant materials for walls, ceilings, and windows?
12.123	Are Uninterruptible Power Supply (UPS) or redundant power sources provided for safety and security of critical equipment, fire detection, alarm and suppression systems; public address; call-for-aid telephones; CCTV; emergency trip stations; vital train control functions; etc.?
12.124	Has the agency removed non-explosive resistant trash receptacles from platform areas of terminals and stations?

12.125	Does the agency employ specific protective measures for all critical infrastructure (e.g., tunnels, bridges, stations, control centers, etc.) identified through the risk assessment particularly at access points and ventilation infrastructure?
12.126	Does the agency have or utilize explosive detection canine teams, either maintained by the system or made available through mutual aid agreements with other law enforcement agencies?
13.000	**Conduct Physical Security Inspections**
13.101	Does the agency conduct frequent inspections of key facilities, stations, terminals, trains and vehicles, or other critical assets for persons, materials, and items that do not belong? Describe frequency of inspection.
13.102	Has the transit agency established procedures for inspecting/sweeping vehicles and stations to identify and manage suspicious items, based on HOT characteristics (hidden, obviously suspicious, not typical) or equivalent system?
13.103	Has the transit agency developed a form or quick reference guide for operations and personnel to conduct pre-trip, post-trip, and within-trip inspections?
13.104	Has the transit agency developed a form or quick reference guide for station attendants and others regarding station and facility inspections?
13.105	Does the system document the results of inspections and implement any changes to policies and procedures or implement corrective actions, based on the findings? Describe specific examples where improvements to policy or procedures have occurred.
13.106	Does the agency conduct frequent inspections of its critical systems access points, ventilation systems, and the interior of underground/underwater assets for indications of suspicious activity?
13.107	Does the system integrate randomness and unpredictability into its security activities to enhance deterrent effect? Describe how.
13.108	Is there a process in place to ensure that in service vehicles are inspected at regular periodic intervals for suspicious or unattended items? Specify type and frequency of inspections.
13.109	Is there a process in place, with necessary training provided to personnel, to ensure that all critical infrastructure are inspected at regular periodic intervals for suspicious or unattended items? Specify type and frequency of inspections.
	BACKGROUND INVESTIGATIONS
14.000	**Conduct Background Investigations of Employees and Contractors**
14.101	Does the agency conduct background investigations on all new front-line operations and maintenance employees, and employees with access to sensitive security information, facilities and systems? (i.e., criminal history and motor vehicle records)
14.102	To the extent allowed by agency policy or law, does the agency conduct background investigations on contractors, including vendors, with access to critical facilities, sensitive security systems, and sensitive security information?
14.103	Has counsel for the agency reviewed the process for conducting employee background investigations to confirm that procedures are consistent with applicable statutes and regulations?
14.104	Does the agency have a documented process for conducting background investigations?
14.105	Is the criteria for background investigations based on employee type and responsibility, and is access documented?
	DOCUMENT CONTROL
15.000	**Control Access to documents of critical systems and facilities**
15.101	Does the agency keep documentation of its security critical systems, such as tunnels, bridges, HVAC systems and intrusion alarm detection systems (i.e. plans, schematics, etc.) protected from unauthorized access?
15.102	Has the agency designated a department/person responsible for administering the access control policy with respect to agency documents?
15.103	Does the security review committee or other designated group review document control practices, assess compliance applicable procedures, and identify discrepancies and necessary corrective action?
16.000	**Process for handling and access to Sensitive Security Information (SSI)**
16.101	Does the agency have a documented policy for identifying and controlling the distribution of and access to documents it considers to be SSI?

16.102	Does the agency have a documented policy for proper handling, control, and storage of documents labeled as or otherwise determined to be SSI?
16.103	Are employees who may be provided SSI materials familiar with the documented policy for the proper handling of such materials?
16.104	Have employees provided access to SSI material received training on proper labeling, handling, dissemination, and storage (such as through the TSA on-line SSI training program)?
	SECURITY PROGRAM AUDITS
17.000	**Audit Program**
17.101	Does the agency have an internal security audit process and has the agency established a schedule for conducting its internal security audit process?
17.102	Does the SSP contain a description of the process used by the agency to audit its implementation of the SSP over the course of the agency's published schedule?
17.103	Has the transit agency established checklists and procedures to govern the conduct of its internal security audit process?
17.104	Is the transit agency complying with its internal security audit schedule?
17.105	Is each internal security audit documented in a written report, which includes evaluation of the adequacy and effectiveness of the SSP element and applicable implementing procedures audited, needed corrected actions, needed recommendations, an implementation schedule for corrective actions and status reporting?
17.106	In the last 12 months, has the Security Review Committee or other designated group addressed the findings and recommendations from the internal security audits, and updated plans, protocols and processes as necessary?
17.107	Does the transit agency’s internal security audit process ensure that auditors are independent from those responsible for the activity being audited?

10

4

9

17

3

10

7

5

26

9

5

3

4

7

170 vs. 222

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 9 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.