

2015

BASELINE ASSESSMENT and SECURITY ENHANCEMENT



The 17 Action Items cover a range of areas including security program management and accountability, security and emergency response training, drills and exercises, public awareness, protective measures for the National Terrorism Advisory System (NTAS) threat levels, physical security, personnel security, and information sharing and security.

1.000 Establish Written System Security Plans (SSPs) and Emergency Response Plan (ERP)

The purpose of the SSP (also referred to as Security and Emergency Preparedness Plan) is to ensure a planned, documented, organized response to actual and potential security threats to the system, and to address these threats with proactive measures and response techniques that manage and minimize the outcome of security breaches or related events.

2.000 Define Roles and Responsibilities for Security and Emergency Management

The purpose of this section is to ensure that agency management and employees are knowledgeable of and well-prepared to develop, disseminate and implement written Security and Emergency Management Plans.

3.000 Ensure that operations and maintenance supervisors, forepersons and managers are held accountable for security issues under their control

The purpose of this section is to ensure that agency front-line supervisors and employees are trained, informed and prepared to implement security and emergency response protocols and procedures appropriate to their function.

4.000 Coordinate Security and Emergency Management Plan(s) with local and regional agencies

The purpose of this section is to enhance and elevate security and emergency preparedness by coordinating, training, exercising and testing agency capabilities with local and regional emergency response agencies.

5.000 Establish and Maintain a Security and Emergency Training Program

The purpose of this section is to ensure that ALL agency personnel are trained, tested and monitored in the current security and emergency response protocols appropriate to their position.

6.000 Establish plans and protocols to respond to the DHS NTAS

The purpose of establishing plans and protocols to respond to information received about imminent or elevated security threats is to ensure a pre-determined, organized response by the Agency, employees and individuals to prevent, mitigate or respond to the threat.

7.000 Implement and reinforce a Public Security and Emergency Awareness program

The purpose of this section is to ensure that the agency develops and implements programs to engage all passengers, contractors and others who come into contact with the system in a program of security awareness activities so that they serve as “eyes and ears” for the system.

8.000 Establish and use a Risk Management Process to assess and manage threats, vulnerabilities and consequences

The purpose of an Agency risk management process is to improve security through a structured, proactive program developed to identify, assess, manage and mitigate the security risks inherent to the system.

9.000 Establish and use an information sharing process for threat and intelligence information

The purpose of this section is to ensure enhanced agency security awareness through formalized information receipt processes and incident/information reporting exchanges to ensure that the

agency has timely, controlled and predictable responses to various types of emergencies that may occur within the system or nearby locations that may impact the system.

10.000 Conduct Tabletop and Functional Drills

The purpose of this section is develop and prepare a coordinated agency emergency response through the conduct of planning, training, exercising and evaluating of response protocols with local and regional first responders.

11.000 Developing a Comprehensive Cyber Security Strategy

The purpose of this section is to enhance agency security awareness and preparedness to identify and protect against cyber security threats to the system.

12.000 Control Access to Security Critical Facilities with ID badges for all visitors, employees and contractors

The purpose of establishing controlled access to identified security critical facilities is to promote protective measures for critical infrastructure essential to uninterrupted / uncompromised system operation.

13.000 Conduct Physical Security Inspections

The purpose of conducting frequent and consistent inspections of security critical facilities, equipment and other critical assets is to ensure prompt identification and resolution of security issues, gaps or conditions.

14.000 Conduct Background Investigations of Employees and Contractors

The purpose of this element is to enhance system security through the conduct and documentation of employee and contractor background investigations based upon identified and verified critical system access requirement levels.

15.000 Control Access to documents of security critical systems and facilities

The purpose of this element is to enhance system security through the identification and protection of employee and contractor document access to critical systems and facilities based upon verified need-to-know access requirements.

16.000 Process for handling and access to Sensitive Security Information (SSI)

The purpose of this element is to enhance system security through the identification and documentation of critical systems and facility access based upon employee and contractor verified access needs requirements.

17.000 Audit Program

The purpose of this element is to assess the effectiveness of the agency's Security Program as related to the inspection, monitoring, auditing and documentation processes and procedures established for all agency functions as well as all of its contractors.