ATNICG/5-WP/23

ATNICG Security

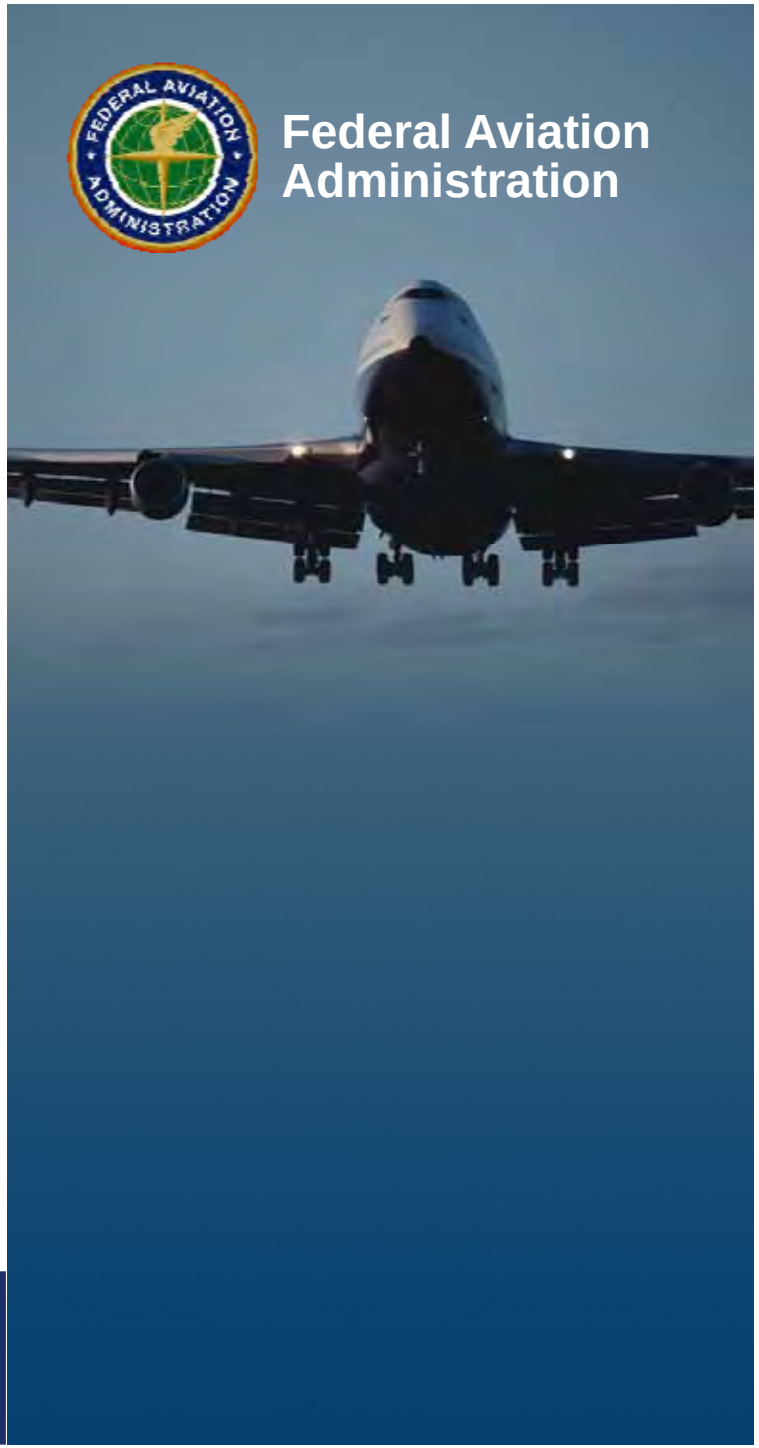
Security Policy, Guidance, and Checklist

ATNICG/5
Kuala Lumpur, Malaysia
31 May – 4 June 2010

Vic Patel

Manager

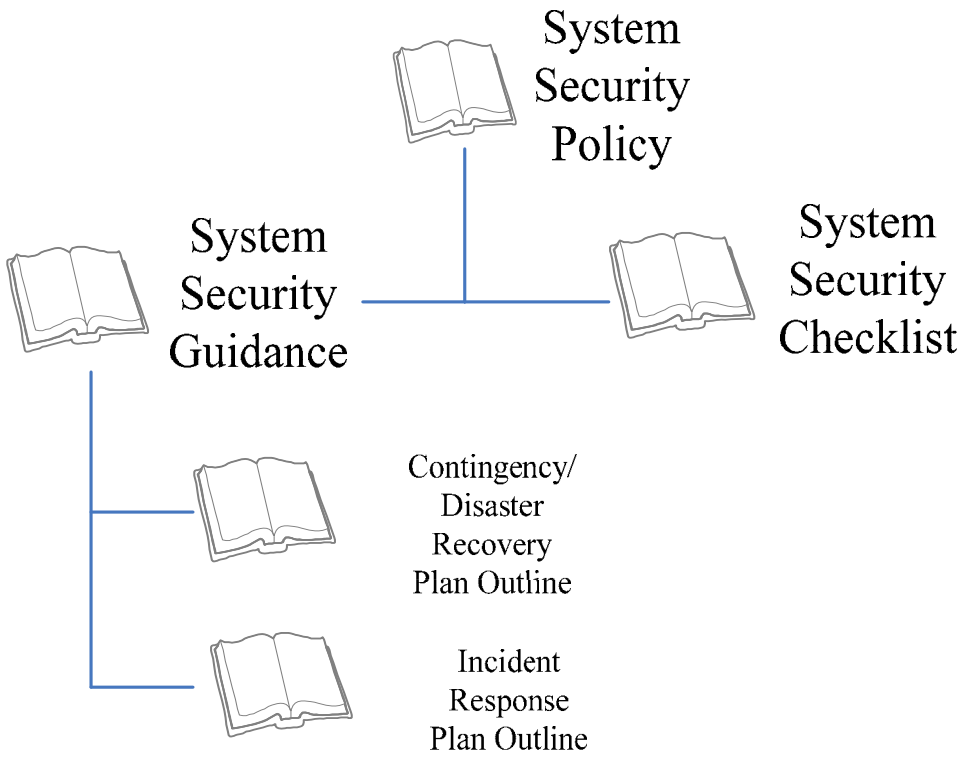
FAA/ATO-P Security Engineering Group



Presentation Overview

- Security Documentation Overview
- System Security Policy
- Security Guidance
  - Security Controls
    - Management, Operational, and Technical Controls
      - Technical Controls for AMHS Security
  - Contingency/Disaster Recovery Plan Outline
  - Incident Response Plan Outline
- System Security Checklist

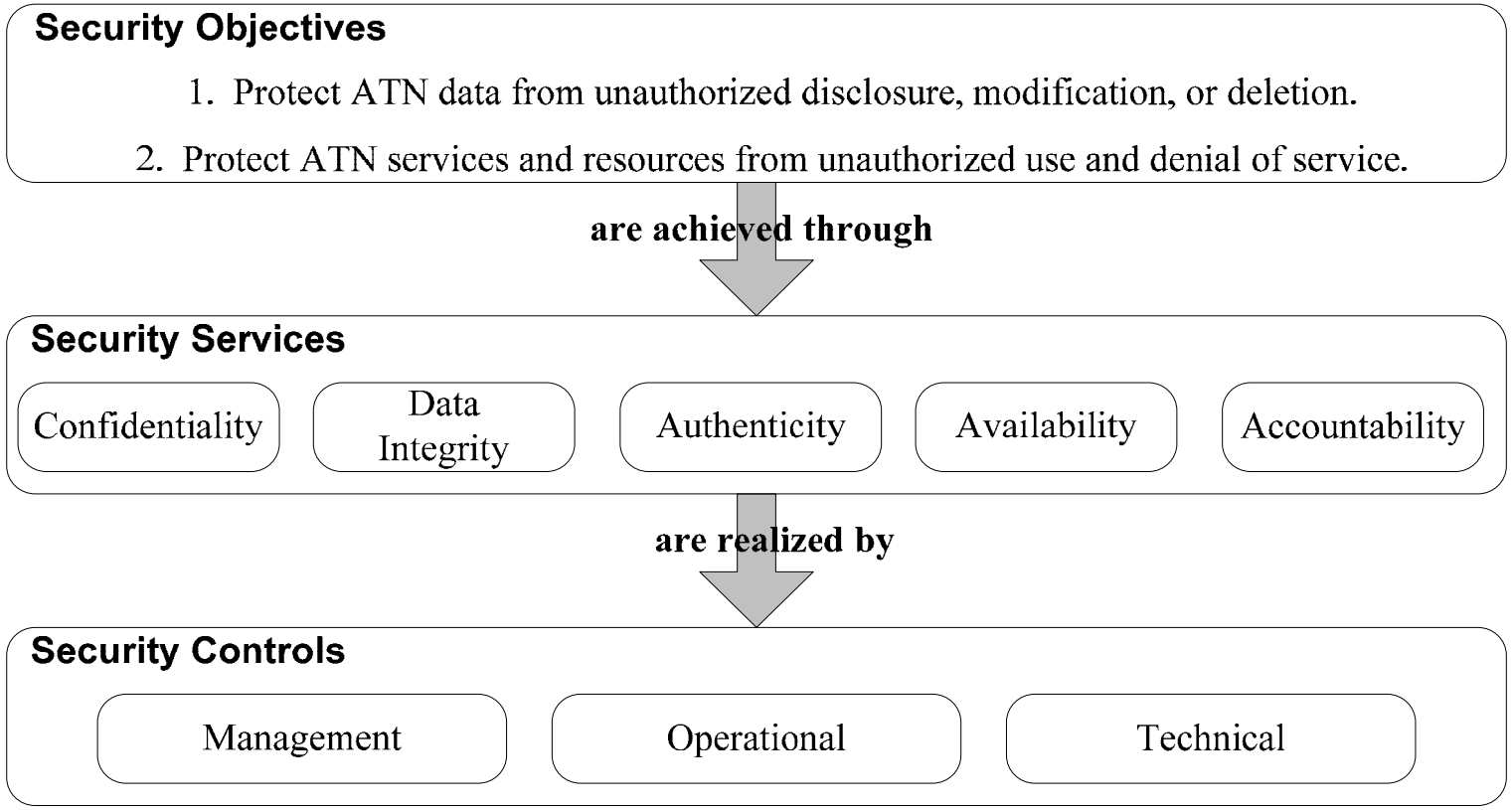
Asia/Pac Security Documentation Overview



System Security Policy

- The policy identifies the following objectives for security:
  - Protect ATN data from unauthorized disclosure, modification, or deletion, and
  - Protect ATN resources from unauthorized use and denial of service.
- The policy identifies the following security services:
  - Confidentiality. Ensures data is not disclosed to unauthorized entities.
  - Data Integrity. Ensures data has not been altered or destroyed in an unauthorized manner.
  - Authenticity. Ensures that the source of data or the identity of an entity is as claimed.
  - Availability. Ensures resources, services, and data are accessible and usable on demand or in a timely, reliable manner by an authorized entity.
  - Accountability. Enables activities to be traced to users and processes that may then be held responsible for those actions.
- The policy requires Verification and Authorization:
  - ATN systems shall be verified to have system security commensurate with the risk and magnitude of harm resulting from unauthorized disclosure, modification, or deletion of ATN data, or unauthorized use and denial of service of ATN services and resources.
  - ATN systems shall be formally approved for operation by the cognizant Designated Approving Authority (DAA).

System Security Guidance
Security Objectives, Services, Controls



System Security Guidance
Security Controls

- Management controls
  - Controls that address management of the security aspects of the system and associated risks
  - Examples are adherence to Security Policy and use of the C&A Checklist
- Technical controls
  - Consists of hardware and software controls used to provide automated protection to the system or applications
- Operational controls
  - Controls that address security mechanisms primarily implemented by people as opposed to systems
  - Examples are Incident Response and Contingency/Disaster Recovery

System Security Guidance
Mapping of Controls onto Policy

Asia/Pac System Security Policy	Technical Controls	Operational Controls	Management Controls
Confidentiality			
(a) ATN data shall be protected from unauthorized disclosure during processing, transmission, and storage commensurate with the designated sensitivity of the data.	System and Communications Protection (SC)	System and Information Integrity (SI) Physical and Environmental Protection (PE)	System and Services Acquisition (SA)
Data Integrity			
(a) ATN data shall be protected from unauthorized or undetected modification during transmission, storage, and processing.	System and Communications Protection (SC)	System and Information Integrity (SI) Physical and Environmental Protection (PE) Configuration Management (CM)	System and Services Acquisition (SA)
Authenticity			
(a) ATN users and processes shall be uniquely identified.	Identification and Authentication (IA)	Peraonnel Security (PS)	
(b) ATN users and processes shall be authenticated before being granted access to ATN data, services, and resources.	Identification and Authentication (IA) Access Control (AC)	Peraonnel Security (PS)	
(c) ATN data, services, and resources shall be protected from unauthorized use or tampering.	Access Control (AC)		
(d) ATN users and processes shall have access only to those ATN data, services, and resources for which they have authorization.	Access Control (AC)		

System Security Guidance
Mapping of Controls onto Policy

Asia/Pac System Security Policy	Technical Controls	Operational Controls	Management Controls
Availability			
(a) ATN data, services, and resources shall be available for use by authorized users and processes.	System and Communications Protection (SC)	System and Information Integrity (SI) Contingency Planning (CP) Incident Response (IR) Physical and Environmental Protection (PE) Peraonnel Security (PS)	System and Services Acquisition (SA)
Accountability			
(a) An audit trail of use of ATN data, services, and resources by ATN users and processes shall be maintained.	Audit and Accountability (AU)	Peraonnel Security (PS)	

System Security Guidance
Mapping of Controls onto Policy

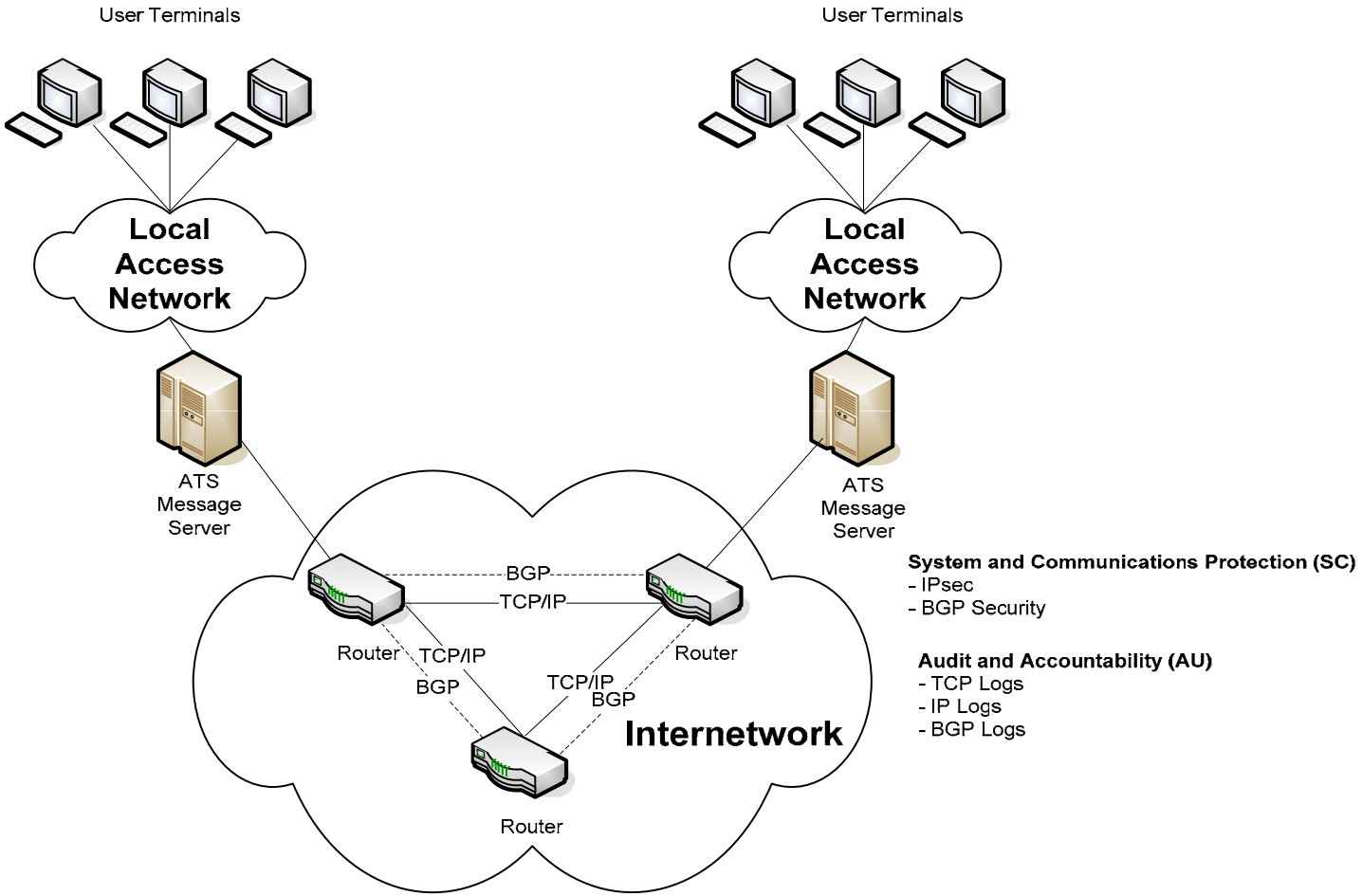
Asia/Pac System Security Policy	Technical Controls	Operational Controls	Management Controls
Verification			
a. ATN systems shall be verified to have system security commensurate with the risk and magnitude of harm resulting from unauthorized disclosure, modification, or deletion of ATN data, or unauthorized use and denial of service of ATN services and resources.			Planning (PL) Risk Assessment (RA)
Authorization			
a. ATN systems shall be formally approved for operation by the cognizant Designated Approving Authority (DAA).			Certification, Accreditation, and Security Assessments (CA)
b. Significant changes to ATN systems shall require another formal approval (or re-authorization).			Certification, Accreditation, and Security Assessments (CA)

System Security Guidance
AMHS Technical Controls

Technical Control Summary

- Technical controls may be applied to secure the communications infrastructure, i.e., to secure router connections
  - Using pre-shared keys
- Technical controls may also be applied to User Agent to MTA Server connections
  - Technique depends on access protocol
- As the AMHS evolves to enhanced services, including directory services, AMHS application security may be employed
- Firewalls and other security appliances should be introduced as needed.
- An incident response and contingency/disaster recovery capability should be introduced along with the technical controls

System Security Guidance
AMHS Technical Controls

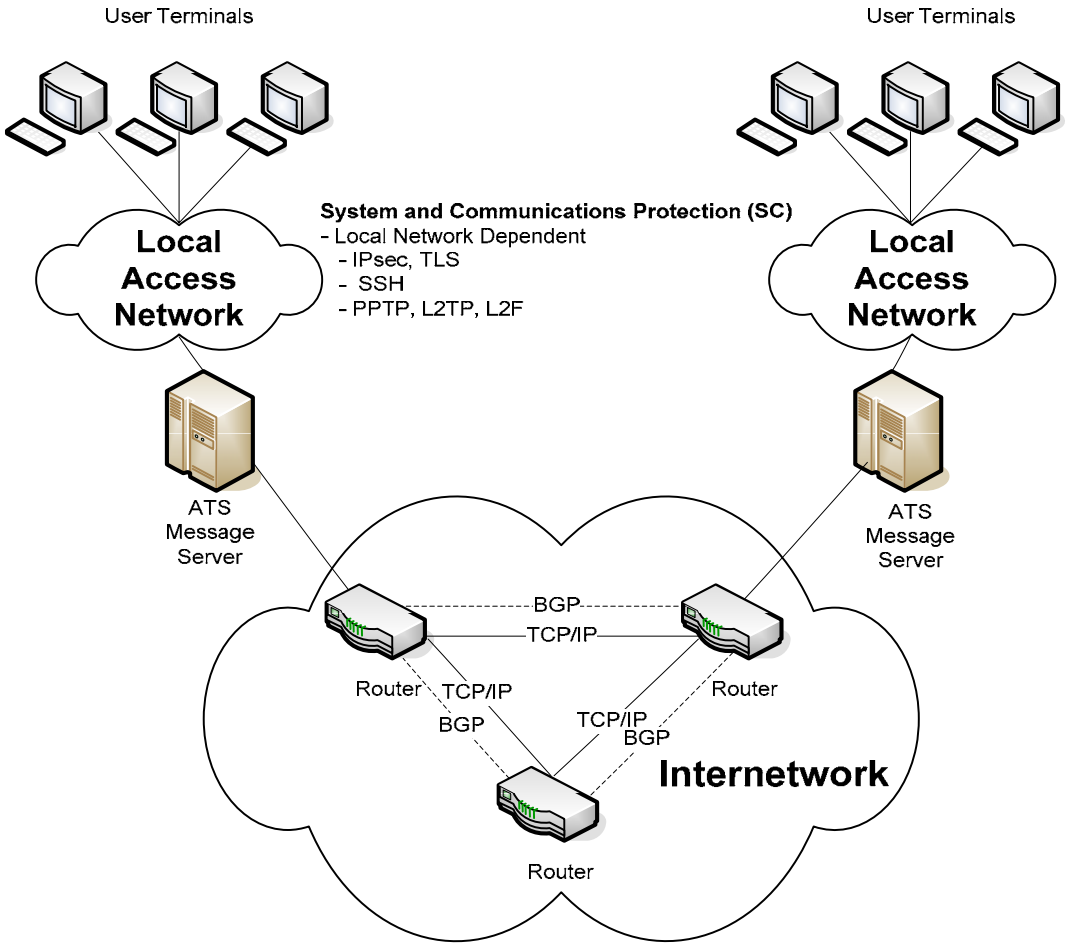


Network Security

Secure Communications between Routers which support MTA Servers

- Communications Security
  - Internet Protocol Security (IPsec)
  - BGP Security
    - TLS
    - Keyed Message Digest (MD-5)
- Audit Logs
  - TCP, IP, BGP Logs

System Security Guidance
AMHS Technical Controls



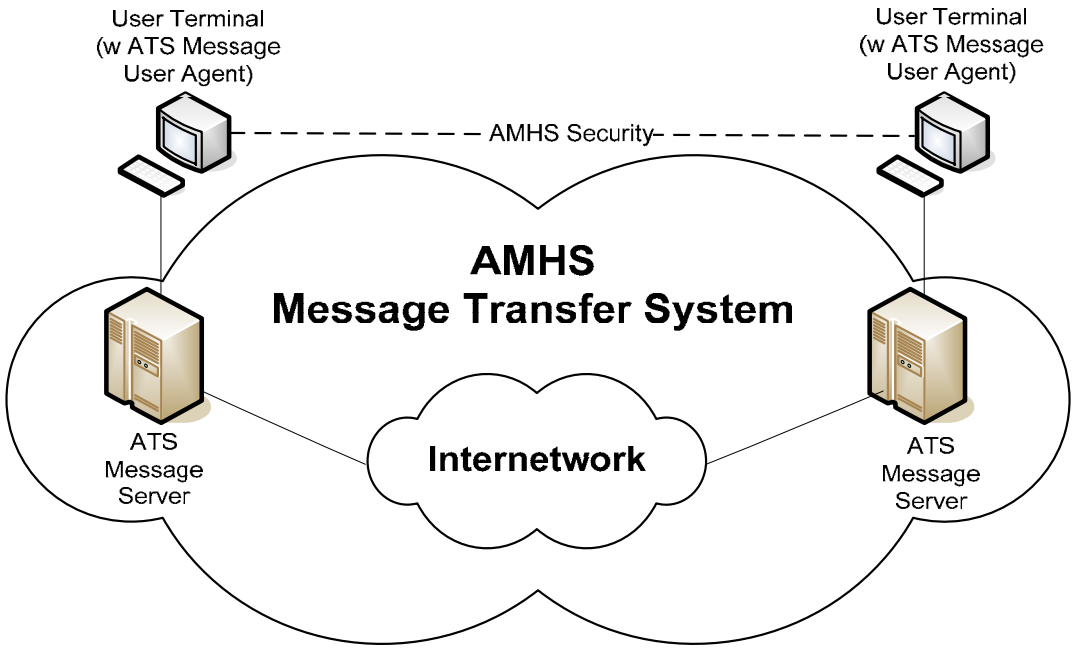
System Security Guidance
AMHS Technical Controls

Secure Communications from User Agents to MTA Server

- Technique depends on connectivity
  - Internet Protocol Security (IPsec)
  - Transport Layer Security (TLS) (formerly Secure Sockets Layer (SSL))
  - Layer 2 Protocols (Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Layer 2 Forwarding (L2F)
  - Secure Shell (SSH)

System Security Guidance
AMHS Technical Controls

System and Communications Protection (SC)
- AMHS Security applied from
  ATS Message User Agent to ATS Message User Agent



System Security Guidance
Contingency/Disaster Recovery Plan

- The System Security Guidance contains an outline for a contingency and disaster recovery plan.

- This plan identifies the coordination activities, processes, and procedures to be followed in the event that an AMHS system is unavailable.

System Security Guidance
Contingency/Disaster Recovery Plan

- NIST SP800-34, Contingency Planning Guide for Information Technology Systems

  "IT contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of IT systems, operations, and data after a disruption. Contingency planning generally includes one or more of the approaches to restore disrupted IT services:

  - Restoring IT operations at an alternate location
  - Recovering IT operations using alternate equipment
  - Performing some or al of the affected business processes using non-IT (manual) means"

System Security Guidance
Incident Response Plan

- The System Security Guidance contains an outline for an Incident Response Plan

- The incident response plan specifies common procedures for identifying, reporting, and responding to computing incidents.

Security Checklist

ID	Security Checklist Text	Implemented (Yes/No)	Comment
	ACCESS CONTROL (AC)		CLASS: TECHNICAL
	ACCOUNT MANAGEMENT		
AC.1	Does the organization manage system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts?		
	ACCESS ENFORCEMENT		
AC.2	Does the system enforce assigned authorizations for controlling access to the system in accordance with applicable policy?		
	SUPERVISION AND REVIEW — ACCESS CONTROL		
AC.3	Does the organization review the activities of users with respect to the enforcement and usage of system access controls?		
	REMOTE ACCESS		
AC.4	Does the organization document, monitor, and control all methods of remote access (e.g., dial-up, Internet) to the system?		
	AWARENESS AND TRAINING (AT)		CLASS: OPERATIONAL
	SECURITY AWARENESS AND TRAINING POLICY		
AT.1	Does the organization have a formal, documented, security awareness and training policy?		
	SECURITY TRAINING		
AT.2	Does the organization provide basic security awareness training to all users?		
	AUDIT AND ACCOUNTABILITY (AU)		CLASS: TECHNICAL
	AUDITABLE EVENTS		
AU.1	Does the system generate audit records for the significant security events?		
	CONTENT OF AUDIT RECORDS		
AU.2	Does the system capture sufficient information in audit records to establish what events occurred, the source of the events (*to hold individual users accountable)*, and the outcomes of the events?		
	AUDIT MONITORING, ANALYSIS, AND REPORTING		
AU.3	Does the organization regularly review/analyze audit records for indications of inappropriate or unusual activity?		

Security Checklist

	CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS (CA)		CLASS: MANAGEMENT
	CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENT POLICY		
CA.1	Does the organization have a formal, documented, security assessment and verification and accreditation policy?		
	SECURITY CERTIFICATION		
CA.2	Does the organization conduct an assessment of the security controls in the system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system?		
	SECURITY ACCREDITATION		
CA.3	Does the organization explicitly authorize (i.e., accredit) the system for operation?		
	CONFIGURATION MANAGEMENT (CM)		CLASS: OPERATIONAL
	CONFIGURATION MANAGEMENT PROCEDURES		
CM.1	Does the organization have formal, documented configuration management policy procedures?		
	CONFIGURATION CHANGE CONTROL		
CM.2	Does the organization control changes to the system?		
	CONTINGENCY PLANNING (CP)		CLASS: OPERATIONAL
	CONTINGENCY PLAN		
CP.1	Does the organization have a formal, documented contingency plan?		
	SYSTEM BACKUP		
CP.2	Does the organization conduct backups of user-level and system-level information?		
	IDENTIFICATION AND AUTHENTICATION (IA)		CLASS: TECHNICAL
	USER IDENTIFICATION AND AUTHENTICATION		
IA.1	Does the system uniquely identify users (or processes acting on behalf of users)?		
IA.2	Does the system authenticate users (or processes acting on behalf of users)?		

Security Checklist

	DEVICE IDENTIFICATION AND AUTHENTICATION		
IA.3	Does the system identify specific devices before establishing a connection?		
IA.4	Does the system authenticate specific devices before establishing a connection?		
	INCIDENT RESPONSE (IR)		CLASS: OPERATIONAL
	INCIDENT RESPONSE PLAN		
IR.1	Does the organization have a formal, documented incident response plan?		
	INCIDENT HANDLING		
IR.2	Does the organization implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery?		
	INCIDENT REPORTING		
IR.3	Does the organization promptly report incident information to appropriate authorities?		
	MAINTENANCE (MA)		CLASS: OPERATIONAL
	CONTROLLED MAINTENANCE		
MA.1	Does the organization perform routine preventative and regular maintenance on the components of the system?		
	MEDIA PROTECTION (MP)		CLASS: OPERATIONAL
	MEDIA ACCESS		
MP.1	Does the organization restrict access to system media to authorized individuals?		
	MEDIA STORAGE		
MP.2	Does the organization physically control system media within controlled areas?		
	PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)		CLASS: OPERATIONAL
	PHYSICAL ACCESS CONTROL		
PE.1	Does the organization control all physical access points to facilities containing systems?		
	EMERGENCY POWER		

Security Checklist

PE.2	Does the organization provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the system in the event of a primary power source loss?		
	FIRE PROTECTION		
PE.3	Does the organization employ and maintain fire suppression and detection devices/systems that can be activated in the event of a fire?		
	PLANNING (PL)		CLASS: MANAGEMENT
	SECURITY PLANNING PLAN		
PL.1	Does the organization have a formal, documented security plan?		
	PERSONNEL SECURITY (PS)		CLASS: OPERATIONAL
	PERSONNEL SECURITY POLICY		
PS.1	Does the organization have a formal, documented personnel security policy?		
	PERSONNEL SCREENING		
PS.2	Does the organization screen individuals requiring access to organizational information and systems?		
	RISK ASSESSMENT (RA)		CLASS: MANAGEMENT
	RISK ASSESSMENT POLICY		
RA.1	Does the organization have a formal, documented risk assessment policy?		
	RISK ASSESSMENT		
RA.2	Does the organization conduct assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and systems that support the operations and assets of the organization?		
	VULNERABILITY SCANNING		
RA.3	Does the organization scan for vulnerabilities in the system?		
	SYSTEM AND SERVICES ACQUISITION (SA)		CLASS: MANAGEMENT
	SYSTEM AND SERVICES ACQUISITION PLAN		
SA.1	Does the organization have a formal, documented system and services acquisition plan?		
	ALLOCATION OF RESOURCES		

Security Checklist

SA.2	Does the organization determine, document, and allocate as part of its capital planning and investment control process the resources required to adequately protect the system?		
	SYSTEM AND COMMUNICATIONS PROTECTION (SC)		CLASS: TECHNICAL
	DENIAL OF SERVICE PROTECTION		
SC.1	Does the system protect against or limit the effects of denial of service attacks?		
	BOUNDARY PROTECTION		
SC.2	Does the system monitor and control communications at the external boundary of the system and at key internal boundaries within the system?		
	TRANSMISSION INTEGRITY		
SC.3	Does the system protect the integrity of transmitted information?		
	TRANSMISSION CONFIDENTIALITY		
SC.4	Does the system protect the confidentiality of transmitted information?		
	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT		
SC.5	Does the system employ automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management?		
	PUBLIC KEY INFRASTRUCTURE CERTIFICATES		
SC.6	Does the organization develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the system?		
	SESSION AUTENTICITY		
SC.7	Does the system provide mechanisms to protect the authenticity of communications sessions?		
	SYSTEM AND INFORMATION INTEGRITY (SI)		CLASS: OPERATIONAL
	SYSTEM AND INFORMATION INTEGRITY POLICY		
SI.1	Does the organization have a formal, documented system and information integrity policy?		
	FLAW REMEDIATION		
SI.2	Does the organization identify, report, and correct system flaws?		
	MALICIOUS CODE PROTECTION		

Security Checklist

SI.3	Does the system implement malicious code protection that includes a capability for automatic updates?		
	SYSTEM MONITORING TOOLS AND TECHNIQUES		
SI.4	Does the organization employ tools and techniques to monitor events on the system, detect attacks, and provide identification of unauthorized use of the system?		
	SECURITY ALERTS AND ADVISORIES		
SI.5	Does the organization receive system security alerts/advisories on a regular basis, issue alerts/advisories to appropriate personnel, and take appropriate actions in response?		
	SOFTWARE AND INFORMATION INTEGRITY		
SI.6	Does the system detect and protect against unauthorized changes to software and information?		
	SPAM AND SPYWARE PROTECTION		
SI.7	Does the system implement spam and spyware protection?		

Questions