AN-Conf/11-IP/39
27/8/03

ELEVENTH AIR NAVIGATION CONFERENCE

Montreal, 22 September to 3 October 2003

Agenda Item 2: Safety and security in air traffic management (ATM)
2.5 Safety and security of the ATM infrastructure :

U.S. SECURITY INFLUENCE ON THE SAFETY OF THE FAA NATIONAL AIRSPACE SYSTEM

(Presented by the United States)

SUMMARY

This paper outlines the security approach to the United States Federal Aviation Administration's National Airspace System, which has a direct impact on safety. The approach is based on three information systems security elements: enterprise security and boundary protection, network security monitoring and incident response, and system security certification and accreditation. The FAA approach is based on international standard and United States developing standards.

REFERENCES

The Federal Information Security management Act, etc.
Computer Security Act of 1987, Public Law 100-235 (H.R. 145), United States Congress, January 8, 1988.
Critical Infrastructure Protection, Presidential Decision Directive 63, William J. Clinton, The White House, May 22, 1998.
Critical Infrastructure Protection, Executive Order, George W. Bush, The White House, October 16, 2001.
Common Criteria of IT Security Evaluation, Version 2.1, ISO International Standard 15408, August 1999.
Information Systems Security Program, Order 1370.82, United States Department of Transportation Federal Aviation Administration, June 9, 2000.
Management of Federal Information Resources, United States Office of Management and Budget (OMB) Circular Number A-130, Transmittal Number 4, November 28, 2000.
Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems, Draft Special Publication 800-37, Version 1.0, United States Department of Commerce, National Institute of Standards and Technology (NIST), October 2002.

1. INTRODUCTION

1.1 Events such as the bombing of the Alfred P. Murrah Federal Building in Oklahoma City and the September 11, 2001 terrorist attacks on the World Trade Center and The Pentagon, as well as other recent events worldwide cyber attacks and the launching of malicious codes such as the Luv Bug and Red Code continue to demonstrate the need to protect and harden infrastructure systems from both physical as well as cyber attack. In response to public law and executive order, the United States government has implemented information system security policies and guidance. Among the body of work resulting from these policies is the Common Criteria, an international standard for applying good security practices to systems.

1.2 As a result of the Year 2000 (Y2K) readiness efforts, significant attention was paid to assuring the continued viability of the national infrastructure. A result of the focus on the national infrastructure was a study revealing that the same infrastructure was vulnerable to accidental and intentional disruption by internal and external physical and cyber threats. The study led the President of the United States to issue Presidential Decision Directive 63 (PDD 63), requiring United States Government agencies to identify and secure their infrastructure systems. The United States Federal Aviation Administration (FAA) responded to PDD 63 by identifying its systems and embarking on a three-year process to certify and authorize its systems (existing and those being acquired) to operate securely within the United States National Airspace System (NAS), based on the Common Criteria international standard, and other United States security policy/guidance issued by the United States National Institute of Standards and Technology (NIST).

1.3 NIST, in cooperation with the United States Department of Defense and the United States National Security Agency has embarked on a mission to develop a single unified security certification and

accreditation guidance document for all United States Government departments and agencies to use. The guidance has been circulated for public comment and is to be finalized in 2004. Its intent is to blend information system security with the system acquisition life cycle. Today, the FAA employs three means to secure the NAS by protecting and assuring the confidentiality, integrity and availability of NAS systems and sub-systems:

a) **Coordinated Security Protection**: In concert with the Office of Safety and Hazardous Materials (ASH), Office of Information Services (AIO), and aeronautical information service (AIS), understanding that a multi-security protection schema is required across most FAA business process these three organization coordinate technology, design, implementation and integration of enhanced security efforts which cross both physical and cyber binderies. The cyber protection aspect is defined as three major information system security (ISS) disciplinary areas consisting of boundary protection, hardening our IT systems from attack and unauthorized use, Identification and Verification of authorized users.

b) **Network Security Monitoring and Incident Response**: Network security monitoring and incident response is handled by FAA's Computer Security Incident Response Center (CSIRC). Operating 24 hours, seven days a week, the CSIRC is responsible for providing information security management for the FAA, and functions as the centralized information assurance management and analysis centre for all NAS, mission support, and administrative systems. The main CSIRC functions are protection, detection, response, and recovery. The basic processes underlying these functions are data collections, data correlation, data analysis, incident response, and recommended solutions.

c) **System Security Certification and Authorization/Accreditation**: To assure safety in the NAS, the FAA focuses considerable attention on the ISS of its NAS resources. In managing its NAS systems, the agency utilizes a formalized ISS process for the following:

1) document system security requirements;

2) conduct system security risk assessments;

3) develop system risk remediation recommendations;

4) develop system security risk mitigation plans;

5) document system security policy and operating procedures; and

6) conduct system security testing.

1.4 This process results in a collection of system security documentation used to formally certify and authorize each system to operate in the FAA NAS. The collection of documents is known as a system Security Certification and Authorization Package (SCAP). The FAA is monitoring ongoing NIST guidance

development activities to synchronize its own Security Certification and Authorization/Accreditation policy and guidance with NIST guidance.

1.5 The safety of the FAA NAS is inseparably linked to the confidentiality, integrity and availability of the NAS systems and sub-systems. A compromise of confidentiality, integrity, and/or availability of NAS systems or sub-systems could represent a serious threat to both revenue and human life. Maintaining the security of the NAS, therefore, has a direct impact on safety.

2. DISCUSSION

2.1 System security certification and accreditation

2.1.1 **Overview**: The current and emerging agency processes rely on the development of a system Risk Assessment which evaluates the system's security requirements, vulnerability, threat and risk, resulting in a set of recommendations to mitigate identified risk. The Risk Assessment forms the heart of the system SCAP, which is developed in accordance with an agency handbook specifying methodology and format. The formal approval process for the SCAP is identified in an agency policy document.

2.1.2 **ISS Standards Developments**: Leveraging commercial products whenever possible to stratify our systems technology refreshments, require that the FAA be a very activity partner in the standards and specification design and development of IT technologies. Additionally the FAA must have direct involvement in the standards formulation of access enabling technologies. It is in this area that the AIS organization has and continues to invest resources to ensure our participation in both national and international standards and specification development bodies. Over the past few years the FAA has been key in the development of PKI, Smart Card and Biometrics standards for international and national machine-readable documents. These standards and specifications are linked to the agencies' efforts in the requirements development and documentation process for our IPTs and commercial acquisitions.

2.1.3 **Requirements Development and Documentation**: As a system is under development, IS security requirements must be documented. An initial risk analysis is performed to determine the initial planned security requirements, which should be documented in a Risk Traceability Matrix. The common document for laying out the desired IS security system environment is the Protection Profile. Once designed, the final design is documented in the Security Target. By this point, the system architecture and anticipated interfaces must be also documented, along with memoranda of agreement/understanding between the system developer/system owner and outside parties who will be interfacing with the system.

2.1.4 **Risk Assessment and Validation Testing**: To assure analysis is independent of system developers and the system owner, an independent Risk Assessment team is formed to review the documented system security requirements, system architecture, system interfaces and operating environment. Following analysis of the system description/architecture and interfaces, the team will tailor an interview outline for the purpose of collecting data. It is essential that data be collected from a broad spectrum of individuals familiar with the system, and those who are involved with the day-to-day operation of the system at a sampling of sites across the country (FAA regional facilities, user facilities, the FAA National Network Control Center (NNCC), vendor service providers and third-party vendors). Data collection may include the use of network scanning tools. Following the analysis of data collected, a Risk Assessment Report is developed. The report

includes comprehensive system/sub-system threat/vulnerability/risk and current risk reduction techniques currently deployed. The findings of the report conclude with recommendations to mitigate any current security risk residing in the system. Following the preparation of the Risk Assessment report, the findings are validated through testing to assure that risks are fully identified in the report.

2.1.5 **System Risk Mitigation and Verification Testing**: Once the Risk Assessment report has been completed, the independent assessment team and the system developer/system owner cooperatively develop a system security Risk Mitigation Plan (RMP) in response to the recommendations made in the Risk Assessment. The RMP provides the system developer's/system owner's prioritized time and cost estimate for mitigating the system's security risks to an acceptable level. Verification testing is performed on each mitigation prior to general deployment, to verify that it does indeed mitigate the system risk, without introducing new or additional risk to the system. If new risks are discovered during testing, the RMP will be updated to reflect changed or additional risk mitigation activity.

2.1.6 **Information System Security and Contingency/Disaster Recovery Planning**: The system developer/system owner is responsible for developing and maintaining a system Information System Security Plan (ISSP) and a system Contingency/Disaster Recovery Plan (C/DRP). The ISSP sets the system security policy determining the system's day-to-day secure operations. The C/DRP details the planning for the steps to take during an event that disrupts service on the system, and the steps to recover from the event. C/DRPs are tested no less than annually to assure their continued efficacy in an emergency.

2.1.7 **Certification and Authorization/Accreditation**: Once the system's security environment is completely documented and tested, a two-step management review and approval process is used to authorize the system's operation in the NAS. The first step is for the system developer/system owner to sign the system certification statement, attesting that the system's security environment has been documented and reviewed in accordance with FAA and United States Government policy. The certification statement is then attached to the system documentation and moved through the management structure for review and approval. Final certification approval is granted by a senior manager in the organization responsible for owning/maintaining the system. Authorization or Accreditation is the next step in the process, which begins with a review by the FAA's information security staff to assure policy has been correctly followed/applied. An authorization statement is drafted by this organization and forwarded to senior management in the agency for review, along with the system security documentation. If approved by senior management, the system will be authorized to operate in the NAS as is, or with the identified mitigation activities pending. In the latter case, a time frame is specified in which the system must be mitigated as planned. This process is required for all systems every three years, or when there is a change in the system's security environment, or when there is a security breech, whichever occurs first.

3. CONCLUSION

3.1 Safety is inseparably linked to system security. The FAA, along with all other United States Government agencies and departments, is now requiring all interconnected systems to be subjected to a formalized ISS review prior to connection. This includes systems owned/maintained by other "trusted" partners or departments. It also includes all leased systems. As ICAO defines its system requirements for systems supporting its member States, security requirements should be identified and built into the systems from the beginning, as well as maintained throughout the systems' life cycle. Assuring that interconnected

systems' security vulnerabilities and risks have been evaluated and mitigated in a standardized process is vital. Following the guidance offered by the Common Criteria will assure such a standardized process is used.

— END —