MTR 98W0000094

MITRE TECHNICAL REPORT

NIMS Information Security Threat Methodology

August 1998

Marshall D. Abrams

Sponsor: Federal Aviation Administration
Dept. No.: F086
Contract No.: DTFA01-93-C-0001
Project No.: 0298014M-NT

Approved for public release; distribution unlimited.

MITRE
Center for Advanced Aviation System Development
McLean, Virginia

MITRE Department
and Project Approval: _____

David G. Hamrick

Abstract

This report presents a methodology for assessing information security threats to the National Airspace System (NAS) Infrastructure Management System (NIMS). Specific vulnerabilities are addressed in a companion report, *Legacy NIMS Vulnerability Study* (FOUO) (Abrams, 1998a). This report is a sanitized version of the MITRE consensus contained in another report, *NIMS Information Security Threats*, (FOUO) (Abrams, 1998b).

Special note for MII readers: The complete report, *NIMS Information Security Threats*, MTR 98W0000089, is controlled distribution available from the author or the F86 Office Coordinator on request.

This sanitized version is made available so that a wider audience may evaluate the applicability of the methodology to their systems. Sanitation has been accomplished by removing the entries in most tables. Some tables have also been deleted.

It is anticipated that the MITRE consensus will be used as a point of departure by an FAA working group to arrive at an official FAA consensus. The relative ability of commercial off-the-shelf (COTS) products in general to counter the threats is identified as an indication of the residual risk in NIMS, which will be built predominantly with COTS products. A comprehensive NIMS risk analysis has not been performed as part of this study.

The analysis employs three threat models: (1) a threat source model, (2) a consequence model, and (3) a primary and secondary threat model. Threat categories are presented at a high level of abstraction, with supporting detail and examples. The results are presented in a table relating 8 threat sources and 15 threat categories. The analysis considers threats experienced by the legacy NIMS, threats expected with the new NIMS, and the anticipated ability of a system implemented from COTS products and meeting the NIMS Protection Profile to resist the identified threats.

KEYWORDS: Information security, NAS, NIMS, threat assessment

Executive Summary

A threat is a circumstance or event with the potential to cause harm to an information system. When discussing threats it is useful to introduce a distinction between *primary threats*—actions that may directly cause damage—and *secondary threats*—actions that may cause countermeasures to fail, thereby allowing those attacks that the primary countermeasures were designed to prevent, detect, or correct. Notice that without primary threats, there can be no secondary threats.

Threats are presented at a high level of abstraction, and are derived from the *NIMS Protection Profile* to ensure coverage. Examples and details are presented in an appendix to explain the high-level statements. These examples are illustrative; they are not intended to be complete or to constitute a full threat taxonomy. The set of examples and causes is unbounded. New flaws and vulnerabilities may be discovered, and new attacks may be invented. Also, technological changes may affect the amount of work necessary for a successful attack.

In this report the term *user* refers to an authorized employee of or contractor to the Airway Facility (AF) organization who employs NIMS as part of his/her duties to manage the National Airspace System (NAS) infrastructure.

As a precursor to a risk assessment, we estimate the ability of COTS products in general to counter the identified threats. A comprehensive risk assessment of NIMS would be necessary to determine the effectiveness of the specific products employed. Also, the influence of the security engineering in adapting and integrating these products into NIMS is at least as important as the specific products selected.

Tables ES-1 and ES-2 provide a format for combining the threats to NIMS with our assessment of the impact of these threats. The tables address the primary and secondary threats, respectively.

Table ES-1. Primary Threats

Primary Threat	Prevalence	COTS Resistance
An unauthorized person may gain logical access to NIMS		
A user, or an unauthorized person masquerading as a user, may gain access to NIMS resources or perform operations for which no access rights have been granted		
Someone may engage in a denial of service attack which may cause the resources of NIMS to be unavailable		
Someone may physically attack NIMS and compromise its information security		

Table ES-2. Secondary Threats

Secondary Threat	Prevalence	COTS Resistance
Security-relevant events may not be recorded or may not be traceable		
Outsiders may intrude on NIMS via its communications capabilities		
Architecture, design, and implementation flaws in NIMS may lead to information security failures		
A system crash may compromise the secure state of NIMS		
Someone may introduce unauthorized software into NIMS		
Someone may tamper with the protection-relevant mechanisms of NIMS		
Improper NIMS administration may cause information security failures		
Improper NIMS operation may cause information security failures		
Changes in the NIMS environment may introduce vulnerabilities		

Acknowledgments

The author acknowledges his debt to MITRE colleagues David G. Hamrick, Susan G. King, Richard P. Stewart, and Joseph M. Veoni who contributed to this report. Special thanks to James G. Williams who formulated the concept of primary and secondary threats.

Table of Contents

List of Tables

Section 1

Introduction

1.1 Purpose and Sensitivity

This report presents a methodology for assessing information security threats to the National Airspace System (NAS) Infrastructure Management System (NIMS). Specific vulnerabilities are addressed in a companion report, *Legacy NIMS Vulnerability Study* (FOUO) (Abrams, 1998a). This report is a sanitized version of the MITRE consensus contained in another report, *NIMS Information Security Threats*, (FOUO) (Abrams, 1998b).

This sanitized version is made available so that a wider audience may evaluate the applicability of the methodology to their systems. Sanitation has been accomplished by removing the entries in most tables. Some tables have also been deleted.

New attack methods and responses constantly emerge. This report focuses on the description of threats at a high level of abstraction to allow us to encompass known and anticipated types of threats; concrete examples are provided to clarify the threat types.

Section 2 presents an overview of three threat models: (1) a threat source model, (2) a consequence model, and (3) a primary and secondary threat model. The details of these models are presented in Appendix B. Section 3 contains the combined threats to NIMS in a table relating 8 threat sources and 15 threat categories with experience of their prevalence in legacy NIMS and expectation of their prevalence in new NIMS. As a precursor to a risk assessment, we estimate the ability of COTS products in general to counter the identified threats. A comprehensive risk assessment of NIMS would be necessary to determine the effectiveness of the specific products employed. Also, the influence of the security engineering in adapting and integrating these products into NIMS is at least as important as the specific products selected.

When the tables are completed, this report would be sensitive because it would identify the threats NIMS may be designed to resist. Malicious attackers might consider this information as a challenge or as identification of a target of opportunity.

1.2 Terminology

Threat and related terms need to be defined to avoid confusion. The best definitions from authoritative sources are:

Threat:

"Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service." (NSTISSI, 1992) Note that a threat does not have to be intentional. Errors and omissions by well-intentioned and authorized personnel are considered threats.

Threat Agent:

"A method used to exploit a vulnerability in a system, operation, or facility." (NCSC TG-004)

Attack:

"Attempt to gain unauthorized access to an Information System's (IS) services, resources, or information or the attempt to compromise an IS's integrity, availability, or confidentiality, as applicable." (NSTISSI, 1992)

Vulnerability:

"A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate system security policy." (NCSC TG-004, 1988)

Risk:

"The expected loss due to, or impact of, anticipated threats in light of system vulnerabilities and strength or determination of relevant threat agents." (NIST, 1992)

Risk management:

"The process concerned with the identification, measurement, control, and minimization of security risks in information systems to a level commensurate with the value of the assets protected." (NSTISSI, 1992)

One additional definition is necessary, but for which no authoritative source could be found:

Threat source:

The person, organization, or circumstance that implements the threat.

1.3 NIMS Security Posture

NIMS is a national sensitive system according to FAA Order 1600.54B, *FAA Automated Information Systems Security Handbook* [FAA, 1989]. A replacement for this FAA Order is in development and has been taken into consideration in developing this report.

1.4 Related Activities and Documents

To put the threat to NIMS threat in context, this section highlights selected contemporary concerns directly relevant to NIMS. Security professionals are moving from a paradigm of risk avoidance to one of risk management. The Executive Branch is mobilizing to protect critical information technology infrastructure. International standards are emerging for information security technology. Additional material is contained in Appendix A.

Table 1. IW Threat Estimate

ORIGIN OF THREAT	KNOWN TO EXIST	PROBABLY EXISTS	LIKELY BY 2005	ONLY AFTER 2005
Incompetent User	Widespread			
Hacker	Widespread			
Disgruntled Employee	Widespread			
Domestic Extremists		Widespread		
Terrorist Group		Limited	Widespread	
Foreign Espionage	Limited		Widespread	
Tactical IW Attack			Limited	Widespread
Strategic IW Attack				Limited

1.4.1 Defense Science Board

In late 1996, the U.S. Defense Science Board published the following information, shown in Table 1, assessing the relative maturity of various Information Warfare (IW) threats (Defense Science Board, 1996, pp. 2-12). Shading in the table indicates "not available" or "not applicable."

By March 1996 the Department of Defense (DOD) had over 2.1 million computers, 10,000 local networks, and 100 long-distance networks. There were over two million DOD computer users, and another two million users who did business with DOD (GAO, 1996). However, vulnerability assessments had been performed on less than 1 percent of all DOD computer systems around the world. As early as 1995 it was estimated that DOD computers were attacked about 250,000 times per year; however, only one in 500 of those attacks was detected and reported. Most DOD computers tested by "controlled" hackers (Red Teams) were easily exploited using "front door" attacks because even the most basic protections were missing. It is not unreasonable to extrapolate similar threats to FAA systems such as NIMS.

1.4.2 Threat References

An extensive library of threat cross references is maintained on the Internet by Fred Cohen & Associates (Cohen, 1998). Top-level topics include threats, attacks, defenses, risk view, organization view, technical view, other views, prevention, detection, reaction, integrity, availability, confidentiality, and an indication of whether the threats are theoretical, demonstrated, or widespread. This list is representative of the threat information available. Detailed descriptions are available for the following threats: activists, club initiates, competitors, consultants, crackers for hire, crackers, customers, cyber-gangs, deranged people, drug cartels, economic rivals, extortionists, foreign agents and spies, global coalitions, government agencies, hackers, hoodlums, industrial espionage experts, information warriors, infrastructure warriors, insiders, maintenance people,

military organizations, nation states, nature, organized crime, paramilitary groups, police, private investigators, professional thieves, reporters, terrorists, tiger teams, vandals, vendors, and whistle blowers.

1.5 Methodology

There is an emerging and developing body of knowledge concerning threats to information systems among information security professionals. Much of this information is anecdotal and continuously evolving. The documents identified in Section 1.4 and Appendix A are representative. There is a paucity of information on which to proceed, especially for a future system. The Office of Management and Budget (OMB) circular A-130 advises that it is not cost-effective to attempt highly quantified determination of threats. Rather, the FAA decided to achieve a consensus among concerned and knowledgeable parties. This report documents the methodology used in formulating MITRE input to that consensus formation.

Section 2

Threat Models

This section provides an overview of three models as a shared conceptual basis and vocabulary for addressing threats applicable to NIMS. Additional detail is found in Appendix B. For additional background, the reader may also wish to consult *An Introduction to Computer Security: The NIST Handbook* (NIST, 1996) and the other references. The threat source model addresses the characteristics of a threat source in terms of objectives, resources and risk tolerance (Salter, 1998). The consequence model addresses the effects of attacks. The primary and secondary threat model differentiates actions that may directly cause damage from those that contribute to reduced effectiveness of security mechanisms.

2.1 Threat Source Model

This model addresses the characteristics of a threat source in terms of objectives, resources, and risk tolerance (i.e., the threat source's willingness to risk detection) as indications of the countermeasures necessary to reduce the system risk to an acceptable level.

A threat source, when choosing to attack, has resource constraints in terms of money, expertise, access, manpower, time, and risk. The threat source expects a positive return on the investment of these resources. That is, the threat source expects to achieve his/her objectives. Some attacks require a great deal of access but not much expertise (e.g., eavesdropping on clear text transmissions on a local area network), while other attacks require a great deal of computational power but no access (e.g., breaking an encryption algorithm). Given the set of all affordable attacks, a rational threat source will choose the attack that maximizes return on investment. Serendipity and irrational behavior should not be ignored, since assuming a rational attacker may be an over-simplification.

Eight threat source categories are identified in this model. An actual threat source may be representative of more than one category. For example, foreign national intelligence agencies may conduct industrial espionage.

- Personnel Errors and Omissions
- Malicious Insider
- National Intelligence
- Information Warrior
- Terrorist
- Organized Crime
- Industrial Espionage
- Hacker

2.2 Consequence Model

This model organizes the common threats by the threat consequences. The threat actions that can cause the consequence are identified in Appendix B.

- **Deception:** Circumstance or event that may result in an authorized user receiving false data and believing it to be true.
- **Disruption:** Circumstance or event that interrupts or prevents the correct operation of services and functions.
- **Usurpation:** Circumstance or event that results in control of services or functions by a threat source.
- **Disclosure:** Circumstance or event in which a threat source gains unauthorized access to data.
- **Fraud and theft:** Circumstance or event in which a threat source profits from an unauthorized action.

2.3 Primary and Secondary Threat Model

When discussing threats it is useful to introduce a distinction between *primary threats* actions that may directly cause damage and *secondary threats* actions that may cause countermeasures to fail, thereby allowing those attacks that the primary countermeasures were designed to prevent, detect, or correct. Notice that without primary threats, there can be no secondary threats. Some examples of primary and secondary threats, and the rationale for their classification, are presented in Tables 2 and 3.

Table 2. Primary Threat Examples

Primary Threat	Rationale
Installing a logic bomb	Causes damage when it goes off
Intrusion by a threat source	Likely to result in damage

Table 3. Secondary Threat Examples

Secondary threats	Rationale
Installing a trap door	Creates the potential for unauthorized, malicious access
Disabling the audit mechanism	Prevents detection of various primary threats

Threats are presented at a high level of abstraction to allow us to encompass known and anticipated types of threats. Examples and details are presented in Appendix B to explain the high-level statements.

2.3.1 Primary Threats to NIMS

- An unauthorized person may gain logical access to NIMS
- A user, or an unauthorized person masquerading as a user, may gain access to NIMS resources or perform operations for which no access rights have been granted
- Someone may engage in a denial of service attack which may cause the resources of NIMS to be unavailable
- Someone may physically attack NIMS and compromise its information security

2.3.2 Secondary Threats to NIMS

- Security-relevant events may not be recorded or may not be traceable
- Outsiders may intrude on NIMS via its communications capabilities
- Architecture, design, and implementation flaws in NIMS may lead to information security failures
- A system crash may compromise the secure state of NIMS
- Someone may introduce unauthorized software into NIMS
- Someone may tamper with the protection-relevant mechanisms of NIMS
- Improper NIMS administration may cause information security failures
- Improper NIMS operation may cause information security failures
- Changes in the NIMS environment may introduce vulnerabilities

Section 3

Threats to NIMS Information Security

3.1 Threat and Risk

Threat resistance is not wholly dependent on automated means. Architecture, physical protection and administrative procedures all contribute. However, this report focuses on the anticipated technical ability of NIMS to resist the identified threats. As mentioned in the introduction, the decision to construct NIMS as much as possible from COTS products has implications for the intensity of threat that can be resisted.

Risk assessment is part of risk management. As a precursor to a risk assessment of NIMS, we estimate the ability of COTS products in general to counter the identified threats. The security engineering involved in integrating these products into NIMS is at least as important as the specific products selected. Several risk assessments will probably be made at key points in the life cycle. An analytical analysis should occur based on a completed design, product selection, and security integration plan. A comprehensive risk assessment must be performed as part of acceptance testing of NIMS to determine the effectiveness of the actual implementation. This assessment, including testing, will identify residual risks that are not countered by the technical, administrative, and procedural safeguards. Authorizing NIMS to process sensitive information will involve acceptance of those residual risks.

3.2 Threat Assessments

Table 4 illustrates combining the threats to NIMS with the assessment of the impact of these threats. The model used to present the threat to NIMS combines the threat sources from the threat model with the threat categories of the primary and secondary threats. The threat consequence model is employed in the analysis. Table 4 applies to all the primary threats and most of the secondary threats. A copy of the table is completed for each primary and secondary threat.

The secondary threat “outsiders may intrude on NIMS via its communications capabilities” excludes errors and omissions by definition; the first row of Table 4 is deleted for this threat. Similarly, the secondary threats “improper NIMS administration may cause information security failures” and “improper NIMS operation may cause information security failures” only address errors and omissions and malicious insiders; only the first two rows of Table 4 are applicable to these threats.

Table 4. Combining Threat Source, Prevalence, and COTS Resistance for Most Threat Sources

Threat Source	Prevalence	COTS Resistance
Errors and omissions		
Malicious Insider		
National Intelligence		
Information Warrior		
Terrorist		
Industrial Espionage		
Organized Crime		
Hacker		

List of References

Abrams, Marshall, 1998a, *Legacy NIMS Vulnerability Study*, The MITRE Corporation, MITRE Technical Report 98W0000052, FOUO controlled distribution.

Abrams, Marshall, 1998b, *NIMS Information Security Threats*, The MITRE Corporation, MITRE Technical Report 98W0000089, FOUO controlled distribution.

Cohen, Fred, 1998, *Threat Profiles and Cross-Reference*, Fred Cohen & Associates, http://all.net/CID/Threat/Threat.xref

Computer System Security and Privacy Advisory Board, March 1992, *1991 Annual Report*, National Institute of Standards and Technology, Gaithersburg, MD, p. 18.

Defense Science Board, November 1996, *Report of the Defense Science Board Task Force on Information Warfare - Defense (IW-D)*, Appendix A, *Threat Assessment*.

Federal Aviation Administration, 1989, *FAA Automated Information Systems Security Handbook*, FAA Order 1600.54B.

Federal Aviation Administration, 1994, *Telecommunications and Information Systems Security Policy*, FAA Order 1600.66.

Federal Aviation Administration, 1997, *National Airspace System (NAS) Infrastructure Management System (NIMS) Protection Profile*, (draft of August 12, 1997 or most recent version).

General Accounting Office (GAO), May 1996, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks,* AIMD-96-84.

National Institute of Standards and Technology (NIST), 1996, *An Introduction to Computer Security: The NIST Handbook,* Special Publication 800-12, also available at http://csrc.nist.gov/nistpubs/800-12/.

National Computer Security Center, Oct. 1988, *Trusted Network, Glossary of Computer Security Terms*, NCSC-TG-004.

National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, 5 June 1992, *National Information Systems Security (INFOSEC) Glossary*.

President's Commission on Critical Infrastructure Protection, 1998, *Critical Foundations: Protecting America's Infrastructures*, GPO stock number 040-000-00699-1, also available at http://www.pccip.gov/report_index.html.

Salter, Chris, *et al*, September 1998, "Toward a Secure System Engineering Methodology," *New Security Paradigms Workshop*, ACM.

Talbert, N., June 1998, "The Cost of COTS," *Computer*, IEEE Computer Society.

White House, The, May 1998, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63.

Appendix A

Related Information Security Activities

A.1 The President's Commission on Critical Infrastructure Protection (PCCIP)

The PCCIP advises and assists the President of the United States by recommending a national strategy for protecting and assuring critical infrastructures from physical and cyber threats. The Commission's report *Critical Foundations: Protecting America's Infrastructures* (PCCIP, 1998) builds a case and provides a strategy for action. When a strategy is implemented, the FAA will be a significant player given its role in the transportation infrastructure. The FAA must continue to balance security, performance, cost, schedule, and other programmatic objectives.

A.2 The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63

Presidential Decision Directive 63 (White House, 1998) explains key elements of the Clinton Administration's policy on critical infrastructure protection. It analyzes U.S. reliance upon certain critical infrastructures and upon cyber-based information systems. Every department and agency of the Federal Government is responsible for protecting its own critical infrastructure, especially its cyber-based systems and for developing a plan for protecting its own critical infrastructure, including its cyber-based systems. The FAA is explicitly tasked to "develop and implement a comprehensive National Airspace System Security Program to protect the modernized NAS from information-based and other disruptions and attacks."

A.3 NIMS Protection Profile

The *NIMS Protection Profile* (FAA, 1997) gives a comprehensive description of the NIMS security environment. The *Protection Profile* presents assumptions, preliminary guidelines, and requirements for information security in NIMS. It clarifies key security concepts, summarizes recent developments in security practices, and relates those developments to NIMS and the NIMS operational environment. The *Protection Profile:*

- Describes the influence of recent work on security criteria and risk-management guidelines and addresses their application to NIMS
- Describes security assurance needs, security policy and principles, and classes of NIMS security threats to be considered
- Summarizes security objectives
- Contains functional requirements for information security policy enforcement
- Contains information security assurance requirements
- Provides a summary of risk management concepts

Appendix B

Threat Model Details

This appendix provides an elaboration of the three threat models introduced in Section 2. These models provide a shared conceptual basis and vocabulary for addressing threats applicable to NIMS. The threat source model addresses the characteristics of a threat source in terms of objectives, resources, and risk tolerance. The consequence model addresses the effects of attacks. The primary and secondary threat model differentiates actions that may directly cause damage from those that contribute to reduced effectiveness of security mechanisms.

The model used in Section 3 to present the threat to NIMS combines the threat sources from the threat model with the threat categories of the primary and secondary threats. The consequences are employed in the analysis.

B.1 Threat Source Model

This subsection addresses the characteristics of a threat source in terms of objectives, resources, and risk tolerance (i.e., the threat source's willingness to risk detection) as indications of the countermeasures necessary to reduce the system risk to an acceptable level.

A threat source, when choosing to attack, has resource constraints in terms of money, expertise, access, manpower, time, and risk. The threat source expects a positive return on the investment of these resources. That is, the threat source expects to achieve his/her objectives. Some attacks require a great deal of access but not much expertise (e.g., eavesdropping on clear text transmissions on a local area network), while other attacks require a great deal of computational power but no access (e.g., breaking an encryption algorithm). Given the set of all affordable attacks, a rational threat source will choose the attack that maximizes return on investment. Serendipity and irrational behavior should not be ignored, since assuming a rational attacker may be an over-simplification.

For applying the threat source model, eight threat source categories were identified: personnel errors and omissions, malicious insider, national intelligence, information warrior, terrorist, organized crime, industrial espionage, and hacker. An actual threat source may be representative of more than one category. For example, foreign national intelligence agencies may conduct industrial espionage.

Errors and omissions by authorized personnel differ from other threats in that there is no intent. However, the occurrence of a security-relevant error or omission can be construed as an attempt, albeit unintentional, to violate the information system's policy. Referring to an incidence of an error or omission as an information security *attack* is similar to referring to an traumatic incidence of heart disease as a *heart attack*. Errors and omissions may be indistinguishable from deliberate insider attacks from a detection viewpoint. Education has some effectiveness as a countermeasure for errors and omissions, but none for deliberate attacks.

- **Personnel Errors and Omissions**
  Errors and omissions are an important threat source. This threat source is differentiated from the malicious insider in that the errors and omissions are unintentional. A long-term survey of computer-related economic losses (Computer System Security and Privacy Advisory Board, 1992) found that 65 percent of losses to organizations were the result of errors and omissions.

  Data and system integrity, availability, and confidentiality can all be adversely affected by errors caused by authorized persons. Many programs lack internal quality control measures. Data errors are insidious and their effects often are not traceable. Data quality assurance (or management) is not universally practiced. Even the most sophisticated programs cannot detect all types of input errors or omissions. This threat source category is extremely common.
- **Malicious Insider**
  The malicious insider is a very dangerous and insidious threat source. The insider often has authorized access to the systems or infrastructures s/he attacks. This allows the insider to ignore some or all of the security measures that might deter an outsider. The insider may have access to a wide range of FAA resources and more opportunities to exploit security weaknesses. The goals of the insider include revenge, financial gain, institutional change, and occasionally publicity for a cause. Malicious insiders may have a very high risk tolerance, because they may believe they are acting for a higher purpose. A successful masquerade attack allows an attacker to operate with the privileges of an insider; therefore, even if it is inconceivable that an insider could become malicious, this threat source category is considered one of the most dangerous.
- **National Intelligence**
  A foreign national intelligence agency may be a very capable and financially well supported threat source. However, such a threat source is highly averse to risk. The well supported national intelligence threat source may use his resources to gain a level of access second only to that of the insider. The objectives of this threat source are to gain long-term political, economic, or military advantage by collecting and distributing information. Obtaining that information may entail actively attacking information, telecommunications, and even physical systems.
- **Information Warrior**
  An information warrior is a military threat source who undermines its target's ability to wage war by attacking the target's information or network infrastructure. Like the foreign national intelligence threat source, an information warrior may have extensive resources. However, the information warrior differs from foreign national intelligence threats in two respects: its focus on reducing the target's ability to wage war and its greater tolerance of short-term risk. The objectives of the information warrior are basically military advantage and chaos. Some of the particular facilities that an information warrior might choose to target include: command and control facilities, telecommunications, logistics and supply

facilities, weapons systems, and transportation lines. Targets may also include civil infrastructure, such as the NAS and NIMS.

- **Terrorist**
  This category of threat source includes a broad range of ideologically-motivated organizations, both foreign and domestic. Most of the threats associated with this category involve attacks on system availability or integrity. The objectives of the terrorist include chaos, publicity, and revenge. Since the terrorist considers that a state of war exists, s/he willingly endures risks detection. Since terrorist groups are typically from third-world countries or are outside the mainstream organizations, they may not have as much money, expertise, or access as a nationally funded intelligence or information war threat source.
- **Organized Crime**
  Organized crime is a type of threat source that identifies and exploits vulnerabilities with the goals of making money and gaining power. As electronic commerce becomes widespread, criminal elements will become more active in cyber attacks. Because this threat source has a stake in preserving the status quo and their place in it their risk tolerance is lower than that of terrorists and information warriors.
- **Industrial Espionage**
  Participants in industrial espionage seek competitive advantage by obtaining the proprietary information of competitors. Their attacks are highly targeted to obtain specific information. A company engaged in industrial espionage will devote the resources necessary to achieve its aims. Since industrial adversaries must preserve their reputation in the business community, their risk tolerance is low.
- **Hacker**
  The hacker is typically defined as an individual with substantial technology expertise, engaged in compromising computer and telecommunication systems for personal pleasure. Their resource level is low and they are risk averse, but they may have unlimited time and no fear of prosecution—often because they don't expect to be detected or don't expect retaliation. Immaturity contributes to their expectations. Hackers may engage in illegal activities without any perceived risk. The primary danger posed by the hacker community is their potential, in aggregate, to erode public trust and confidence in public infrastructures.

Each class of threat source is given a rating of high, medium, or low for resources and risk tolerance:

- **Resources:** Resources includes the money, technical expertise, and access available to a threat source. Note that if a threat source has a lot of money but not much technical sophistication (like a drug cartel), then the threat source can simply buy the necessary expertise (like drug cartels do).

- A **High** resource rating indicates that the threat source has the money or expertise normally associated with a national level organization, say, an annual budget in the hundreds of millions of dollars.
- A **Medium** resource rating indicates the money or expertise associated with large corporations, say, a budget in the millions of dollars.
- A **Low** resource rating indicates financial or technical resources typically associated with small organizations or individuals, say, a budget less than a million dollars.

- **Risk Tolerance:** A threat source's level of risk tolerance is the severity of the consequences of being caught that the threat source is willing to accept. Desperation, fear, retaliation, exposure, and the opportunity for future attacks all factor into the threat source's risk tolerance.
  - A **High** rating in risk tolerance indicates a very desperate threat source, willing to accept any consequence in order to carry out his mission. Often, adversaries willing to incur this amount of risk consider themselves in a state of war.
  - - A **Medium** rating in risk tolerance indicates a threat source willing to risk his job, or serve jail time, but might not be willing to risk his life.
  - - A **Low** rating in risk tolerance indicates a threat source who is not willing to risk personal harm or who does not believe the chance of harm is great.

Table B-1 summarizes the threat source characteristics. In the table, access takes into account the likely effectiveness of available countermeasures.

Table B-1. Threat Source Characteristics

Threat Source	Objectives	Money	Expertise	Access	Risk Tolerance
Errors & Omissions	None	↓	↑	↑	↑
Malicious Insider	Revenge, retribution, financial gain, institutional change	↓	↑	↑	–
National Intelligence	Information, political military, and economic advantage	↑	↑	–	↓
Information Warrior	Military advantage, chaos, damage to target	↑	–	–	↓
Terrorist	Visibility, publicity, chaos, political	–	↓	↓	↑

Threat Source	Objectives	Money	Expertise	Access	Risk Tolerance
	change				
Industrial Espionage	Competitive advantage	–	–	–	↓
Organized Crime	Monetary gain	–	↑	–	–
Hacker	Thrill, challenge, prestige, notoriety	↓	–	↑	↓

Key: ↑ high – medium ↓ low

B.2 Consequence Model

This model provides an overview of common threats applicable to NIMS, organized by the threat consequences and threat actions. The threat consequences are deception, disruption, usurpation, disclosure, fraud, and theft. Some of the threat actions appear under multiple consequences. These consequences and actions were used in the analysis reported in Section 3.

- **Deception:** Circumstance or event that may result in an authorized user receiving false data and believing it to be true.
  - **False Denial of Origin:** Action in which the originator of data denies responsibility for its generation.
  - **False Denial of Receipt:** Action in which the recipient of data denies receiving and possessing the data.
  - **Falsification:** Action whereby false data deceives authorized user.
  - **Insertion:** Action whereby an authorized user is deceived by the introduction of false data.
  - **Malicious Logic:** In context of masquerade, any hardware, firmware, or software (e.g., Trojan horse) that appears to do a useful or desirable task, but actually gains unauthorized access to infrastructure resources or tricks a user into executing other malicious logic.
  - **Masquerade:** Action whereby a threat source gains access or performs malicious act by posing as an authorized user.
  - **Repudiation:** Action where by a threat source deceives an authorized user by falsely denying responsibility for an act.
  - **Substitution:** Action in which valid data is altered or replaced with false data that serves to deceive an authorized user.
- **Disruption:** Circumstance or event that interrupts or prevents the correct operation of services and functions.
  - **Hardware or Software Error:** Error that causes failure of critical system component(s) and leads to disruption of operation.

- **Hardware or Software Error:** Hardware or software action or inaction that results in the modification of functions or data.
- **Human Error:** Human action or inaction that results in the modification of functions or data. Action or inaction that disables system component(s).
- **Incapacitation:** Action in which infrastructure operation is prevented or interrupted due to the disabling of critical system components.
- **Interference:** Action that disrupts operations by blocking communications of user data or control information.
- **Malicious Logic:** In context of corruption, any hardware, firmware, or software (e.g., a virus) intentionally introduced into the infrastructure to modify critical system functions or data.
- **Malicious Logic:** In context of disabling, any hardware, firmware, or software (e.g., time bomb) intentionally introduced into the infrastructure to destroy critical system functions or data.
- **Natural Catastrophe:** Any "act of God" (e.g., fire, flood, wind, or earthquake) that disables critical infrastructure component(s).
- **Obstruction:** Action in which delivery of services is interrupted by hindering operations.
- **Overload:** Action that hinders operation by placing an excess burden on the performance capabilities of infrastructure elements.
- **Physical Destruction:** Action that deliberately destroys critical components to interrupt or prevent infrastructure operation.
- **Tampering:** In context of corruption, deliberate modification of logic, data, or control information to interrupt or prevent correct operation of critical functions.

- **Usurpation:** Circumstance or event that results in control of services or functions by a threat source.
  - **Malicious Logic:** In context of misuse, any hardware, software, or firmware intentionally introduced into the infrastructure to perform or control execution of an unauthorized function or service.
  - **Misappropriation:** Action in which a threat source assumes logical or physical control of a resource, component, or service.
  - **Misuse:** Action that causes elements to perform a function or service that is detrimental to security.
  - **Tampering:** In context of misuse, deliberate modification of logic, data, or control information to cause the system to perform unauthorized functions or services.
  - **Theft of Data:** Unauthorized acquisition and use of data.
  - **Theft of Service:** Unauthorized use of service by a threat source.
  - **Violation of Permissions:** Action by an user that exceeds the user's privileges by executing an unauthorized function.

- **Disclosure:** Circumstance or event in which a threat source gains unauthorized access to data.
  - **Cryptanalysis:** Technique for converting enciphered data into plaintext without prior knowledge of variables or algorithms used in encipherment process.
  - **Eavesdropping:** Monitoring and recording data by intercepting data other than on a physical link, such as in a host or relay.
  - **Exposure:** Action involving release of sensitive data to a threat source.
  - **Hardware or Software Error:** System failure that results in a threat source receiving unauthorized knowledge of sensitive data.
  - **Human Error:** Human action or inaction that unintentionally results in a threat source receiving unauthorized knowledge of sensitive data.
  - **Inference:** Action whereby a threat source derives knowledge of sensitive data by reasoning from data that is not sensitive.
  - **Interception:** Action in which a threat source accesses sensitive data traveling between authorized source and destination.
  - **Intrusion:** Action in which threat source gains access to sensitive data by circumventing security protections.
  - **Penetration:** Action in which unauthorized logical access to sensitive data is gained by circumventing information technology protections.
  - **Reverse Engineering:** Process whereby sensitive data is acquired by disassembling and analyzing the design of an infrastructure component.
  - **Scavenging:** Process of searching through system residue to acquire unauthorized knowledge of sensitive data.
  - **Theft:** Gaining access to sensitive information by stealing physical media (e.g., tapes, disks) that contains data.
  - **Traffic Analysis:** Technique whereby a threat source gains indirect knowledge of sensitive data transmitted on a communications link without actually reading transmitted data.
  - **Trespass:** Action in which unauthorized physical access to sensitive data is gained by circumventing physical protections.
  - **Wiretapping:** Monitoring and recording data while it is being transmitted on a physical medium.
- **Fraud and theft:** Circumstance or event in which a threat source profits from an unauthorized action. Fraud and theft can be committed by insiders or outsiders. Insiders (i.e., authorized users of a system) are responsible for the majority of fraud. Computer systems can be exploited for both fraud and theft both by automating traditional methods of fraud and by using new methods. Present and former employees, with their knowledge of operations and program flaws, may pose a threat. Computer hardware and software may also be vulnerable to theft.

B.3 Primary and Secondary Threat Model

A threat is a circumstance or event with the potential to cause harm to an information system. When discussing threats it is useful to introduce a distinction between *primary threats*—actions that may directly cause damage—and *secondary threats*—actions that may cause countermeasures to fail, thereby allowing those attacks that the primary countermeasures were designed to prevent, detect, or correct. Notice that without primary threats, there can be no secondary threats. Some examples of primary and secondary threats, and the rationale for their classification, are presented in Tables B-2 and B-3.

Threats are presented at a high level of abstraction and are derived from the *NIMS Protection Profile* to ensure coverage. Examples and details identified in Appendix 2 of FAA Order 1600.66, *Telecommunications and Information Systems Security Policy* (FAA, 1994), are presented to explain the high-level statements. Section numbers are included in parentheses for those examples extracted from FAA Order 1600.66. Some examples may appear under more than one high-level threat or may appear more than once in FAA Order 1600.66 in slightly different form.

These examples are illustrative; they are not intended to be complete or to constitute a taxonomy. The set of examples and causes is unbounded. New flaws and vulnerabilities may be discovered. New attacks may be invented. Technological changes may affect the amount of work necessary for a successful attack.

Table B-2. Primary Threat Examples

Primary Threat	Rationale
Installing a logic bomb	Causes damage when it goes off
Intrusion by a threat source	Likely to result in damage

Table B-3. Secondary Threat Examples

Secondary threats	Rationale
Installing a trap door	Creates the potential for unauthorized, malicious access
Disabling the audit mechanism	Prevents detection of various primary threats

B.3.1 Primary Threats

The following subsections identify, for each primary threat class, common threat sources, likely causes (i.e., technical or organizational vulnerabilities), and specific threat actions that cause harm or loss. The primary threats are:

- An unauthorized person may gain logical access to NIMS
- A user, or an unauthorized person masquerading as a user, may gain access to NIMS resources or perform operations for which no access rights have been granted
- Someone may engage in a denial of service attack which may cause the resources of NIMS to be unavailable
- Someone may physically attack NIMS and compromise its information security

B.3.1.1 An Unauthorized Person May Gain Logical Access To NIMS

This threat is a form of masquerade by individuals that impersonate authorized users. Common threat sources include people outside the organization, hackers, hostile intelligence agents, industrial espionage agents, terrorists, and ex-employees (1b)

Specific causes include:

- Lax security enforcement (e.g., inadequate authentication) (2d4b, 4e3b)
- User carelessness
- NIMS failure to adapt to changes in the threat environment

Specific attack methods include:

- Interception of NIMS internal communications
- Interceptions of communications between NIMS and other FAA hosts
- Impersonation (e.g., via password guessing) (2c1, 3b1)
- Off-line password guessing (2g2, 3d10b)
- Autodialer scanning (2g3, 3d10c)
- Exploiting inadequate authentication (4e3b)

B.3.1.2 A User, Or An Unauthorized Person Masquerading As A User, May Gain Access To NIMS Resources Or Perform Operations For Which No Access Rights Have Been Granted

Common threat sources are people within the organization. This includes individuals who intentionally or unintentionally violate the integrity of the system (1a)

Specific causes include:

- Inadequate access control

- Incorrect setting of security attributes
- Masquerade and stealing of user's rights

Specific threat actions include:

- Passive observation exposure (2a1)
- Scavenging (2a2)
- Deliberate disclosure (2d1)
- Exploiting inference and aggregation vulnerabilities (e.g., reverse engineering) (2d3, 3d6)
- Exploiting product vulnerabilities, (e.g., exploiting covert channels) (2d4a)
- Inappropriate disclosure threats, browsing, searching for exploitable patterns (2e)
- Inappropriate disclosure, preparation for misuse; code-breaking efforts (2g1, 3d10)
- Deliberate compounding of small errors (3d7)
- Misapplication of software, application to wrong data (3e3a)
- Misapplication of software, miscommunication of inputs (3e3b)

B.3.1.3 Someone May Engage In A Denial Of Service Attack Which May Cause The Resources Of NIMS To Be Unavailable

Common threat sources include automated NIMS components, users, and outsiders.

Specific causes include:

- Lack of resource availability
- Failure of resource-assuring measures
- Inappropriate use of security parameters

Specific attacks include

- Denial-of-service attacks
- Loss Of Service Threats, Usage threats; Overload
- Normal excess usage (4e12a)
- Runaway programs (4e12b)
- Overload-Personal use of organization computers (4e12c)

B.3.1.4 Someone May Physically Attack NIMS And Compromise Its Information Security

Common threat sources include inanimate agents. This includes such things as routine water damage, power surges and failures, physical calamities, hardware failure within the information technology (IT) product, malfunctioning external devices and systems, and disabled external devices and systems (1c). Specific causes include inadequate physical protection.

Specific attacks include:

- Theft of physical media (2b1)
- Physical trespass and observation (2b2)
- Implanting eavesdropping devices (2b3)
- Disarming controls (e.g., via routine maintenance) (2b4)
- Implanting malicious hardware (3a1)
- Disarming hardware controls (3a2)
- Deliberate hardware modification (4b1)
- Disabling critical components (4b2)
- Shutting off system or power supply (4b3)
- Implanting self-destruct devices (4b4)
- Routine maintenance (4c2)
- Accidental damage (e.g., water damage) (4c3)
- Interference (e.g., electronic jamming) (4d)
- Deliberate denial of service (4e1)

B.3.2 Secondary Threats

In contrast to primary threats, secondary threats do not normally involve identified loss or harm. The secondary threats are:

- Security-relevant events may not be recorded or may not be traceable
- Outsiders may intrude on NIMS via its communications capabilities
- Architecture, design, and implementation flaws in NIMS may lead to information security failures
- A system crash may compromise the secure state of NIMS
- Someone may introduce unauthorized software into NIMS
- Someone may tamper with the protection-relevant mechanisms of NIMS

- Improper NIMS administration may cause information security failures

- Improper NIMS operation may cause information security failures
- Changes in the NIMS environment may introduce vulnerabilities

B.3.2.1 Security-Relevant Events May Not Be Recorded Or May Not Be Traceable

Common threat sources include both authorized users and outsiders. Specific causes include:

- Mismanagement of the audit facility
- Scope of audit requested
- Insufficient integration of audit trails
- Audit storage exhaustion
- Other inadequacies of the audit mechanism
- User negligence (e.g., failing to log out when leaving a workstation) (2f)
- Failure to properly audit a user action opens the possibility of repudiation (falsely denying origin or receipt of information) (3d2)

B.3.2.2 Outsiders May Intrude On NIMS Via Its Communications Capabilities

Specific threat actions include:

- Eavesdropping (2a3)
- Wiretapping (2a4)
- Traffic analysis (2a5)
- Other forms of signals intelligence (2a7)

B.3.2.3 Architecture, Design, And Implementation Flaws In NIMS May Lead To Information Security Failures

Such flaws may be introduced or used by NIMS developers, by careless or ill-intended users, and by outsiders masquerading as authorized users.

Specific exploits and corresponding causes include:

- Faulty reuse of objects or devices (2d4e, 3d8e)
- Inadequate argument validation (2d4f, 3d8f)
- Miscellaneous logic errors (2d4g, 3d8g)
- Hardware flaws (2d4h, 3d8h)
- Exploiting covert channels (3d8a)
- Inadequate authentication (3d8b)

- Trap doors that bypass system checks (3d8c)
- Malfunctioning hardware (via aging, routine maintenance) (3a3)
- Inadequate deadlock avoidance (4a1)
- Inadequate response to transient errors (4a2)
- Exploiting product vulnerabilities (4e3)

B.3.2.4 A System Crash May Compromise The Secure State Of NIMS

Note that a crash is regarded as a primary threat with respect to availability and as a secondary threat with respect to other security policies.

Specific causes include improper initialization or recovery (2d4d, 3d8d, 4e3d)

Exploits associated with these vulnerabilities include:

- Inappropriate disclosure threats, misuse of authority
- Fault-and-error threats (integrity violations), misuse of authority
- Loss of service threats, usage threats

B.3.2.5 Someone May Introduce Unauthorized Software Into NIMS

Likely threat sources include malicious or well-intended users, maintenance personnel, and outsiders. A likely cause of these threats is inadequate operational configuration management.

Specific losses and associated attacks include:

- Masquerade (e.g., Trojan horses) (2c2, 3b2, 4e4)
- Trap doors that bypass system checks (2d4c)
- Creating, planting, and arming malicious software (2g4, 3d10d, 4e5)
- Deliberate falsification via data entry of modification (3d1)
- Accidental falsification via data entry or modification (3e1)

B.3.2.6 Someone May Tamper With The Protection-Relevant Mechanisms Of NIMS

Likely threat sources include administrators and outsiders masquerading as ordinary users.

Specific losses and associated attacks include:

- Disarming controls (e.g., via routine maintenance) (2b4)

- Deliberate hardware modification (4b1)
- Disabling critical components (4b2)

B.3.2.7 Improper NIMS Administration May Cause Information Security Failures

The threat sources here are the administrators. Some administrative attacks are highly leveraged and can have a wide variety of effects, others are more narrow in scope.

Specific causes include:

- Misuse of authentication data (e.g., editing password files) (2deb, 3d5, 4e2b)
- Improper setting or modification of object security attributes (e.g., access control attributes) (2d2a, 3d4, 4e2a, 4e10)
- Improper setting or modification of user security attributes (e.g., user privileges)
- Mishandling of encryption keys
- Installing flawed application software (3e2)
- Improper runtime environment (3e3c)
- Willful neglect and other errors of omission (4e6)
- Failure to order necessary supplies (4e7)
- Failure to perform routine maintenance (4e8)
- System shutdown (4e9a)
- Disabling user accounts (4e9b)
- Accidental deletion of critical data (4e11)

B.3.2.8 Improper NIMS Operation May Cause Information Security Failures

Specific causes include:

- Non-compliance with policy and procedures
- Errors, omissions, or malice by users or operators

B.3.2.9 Changes In The NIMS Environment May Introduce Vulnerabilities

Specific causes and examples include:

- Newly discovered vulnerabilities or new attacks could render existing security tactics obsolete or even counterproductive
- Normal aging (4c1)

Glossary

AF	Airway Facilities
COTS	commercial off-the-shelf
DOD	Department of Defense
FAA	Federal Aviation Administration
FOUO	For Official Use Only
GAO	General Accounting Office
INFOSEC	Information Security
IS	Information System
IT	Information Technology
NAS	National Airspace System
NCSC	National Computer Security Center
NIMS	NAS Infrastructure Management
NIST	National Institute of Standards and Technology
NSTISSI	National Security Telecommunications and Information Systems Security Institution
OMB	Office of Management and Budget
PCCIP	President's Commission on Critical Infrastructure Protection