DoD Insider Threat Mitigation

Final Report

of the

Insider Threat Integrated Process Team

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 00000000	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle DoD Insider Threat Mitigation	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) DOD	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms "IATAC COLLECTION"	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 69	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
		Report

4. TITLE AND SUBTITLE
DoD Insider Threat Mitigation

5. FUNDING NUMBERS

6. AUTHOR(S)
DoD

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

14. SUBJECT TERMS
Insider Threat

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

(this page is intentionally blank)

Executive Summary

This report provides an explicit set of recommendations for action to mitigate the insider threat to DoD information systems. The report results from the actions of an Insider Threat Integrated Process Team (IPT) requested by the Senior Civilian Official (SCO) of the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) OASD (C3I). The Team's charter was "to foster the effective development of interdependent technical and procedural safeguards" to reduce malicious behavior by insiders.

The "insider" is anyone who is or has been authorized access to a DoD information system, whether a military member, a DoD civilian employee, or employee of another Federal agency or the private sector. Some recommendations, however, address the broader scope of "system components" or "computer software code" inside a system and intended to carry out a malicious act.

The insider threat is real, and very likely significant. A recent DoDIG report indicates that, for one set of investigations, 87 percent of identified intruders into DoD information systems were either employees or others internal to the organization. Basic sources of insider security problems are 1) maliciousness, 2) disdain of security practices, 3) carelessness, and 4) ignorance of security policy, security practices and proper information system use.

Key elements of a strategy to minimize the impact of the insider threat are:

- Establish criticality – what assets are critical to the mission?
- Establish trustworthiness – seek to reduce the threat by establishing a high level of assurance in the trustworthiness of people, practices, systems and programs
- Strengthen personnel security and management practices
- Protect information assets – by controlling asset sharing, isolating information and capabilities on a need-to-know, identifying and reducing known vulnerabilities, and employing and enforcing effective security policies
- Detect problems
- React/respond

"Vigilance, Now" identifies near-term, high impact recommendations that emphasize security awareness and personal accountability, use of existing protection technologies, and deterrence through publicizing the consequences of misuse, abuse and malicious activity. "Vigilance, Looking Forward from a Strong Foundation" emphasizes practicing security basics, first. It further emphasizes measurably improving personnel management practices, development of a DoD Personnel Security Strategic Plan, reinforcing the need for heightened security awareness, and using available technologies while investing in technology that increases an adversary's risk, cost and work factor to perpetrate malicious actions.

Specific recommendations to implement this strategy are provided in seven categories. Many of these recommendations are deliberately aimed at short-term "fixes" that can be implemented soon. Others recommend medium-term or long-term research programs needed to solve the more fundamental problems.

This report provides the basis for steps that can be taken now to employ a risk management strategy and mitigation plan aimed specifically at the insider threat to DoD information systems.

(this page is intentionally blank)

Table of Contents

1. The Insider Threat

1.1 Tasking and Scope

The Senior Civilian Official (SCO) of the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) OASD (C3I) established[1] the Insider Threat Integrated Process Team (IPT) "to foster the effective development of interdependent technical and procedural safeguards" to reduce the malicious behavior by insiders. The tasking requires the IPT to "recommend actions and policies that lead to establishing comprehensive security, acquisition and personnel practices to address the Insider Threat." The tasking describes insiders as "individuals or organizational entities who have authorized physical or electronic access to Department of Defense (DoD) information and infrastructure resources." "Threat refers to the ability of such individuals or organizational entities to exceed or abuse their authorized access to such resources to exploit, attack or otherwise adversely affect DoD information systems."

The tasking memo identifies five objectives required to counter the insider threat.

- Define and enforce limits on overt access
  - Accountability for actions through reliable (non-refutable) records of actions
  - Review of recorded actions
- Detection of unauthorized activity
- Deterrence
- Mitigation of unauthorized activity
- Response to unauthorized activity

1.2 The Final Report of the Insider Threat IPT

This Final Report presents:

- Background on and framework for understanding the insider threat (Section 2)
- A Template for Action (Section 3)
- The recommendations and findings of the Insider Threat IPT (Appendix A)
- A glossary (Appendix B) and list of Acronyms used (Appendix C)

1.3 Report Structure and Evolution

The report is structured to accommodate changes to recommendations as threats, vulnerabilities, methods and technology, countermeasures and risks evolve.

(this page is intentionally blank)

2. Framework

2.1 The Environment

The Department depends increasingly upon information systems to improve organizational effectiveness and efficiency. Enormous processing power and interconnected information systems have become commonly available. This high capacity work environment enables the insider to access, correlate and associate more information from more numerous information sources than ever before. The deployment of vastly more capable tools has not changed individual security responsibilities. The Department requires each insider to protect DoD information and information systems aided by of a variety of physical, procedural, and information technology measures approved by information system Designated Approving Authorities.

2.2 The Insider

The "insider" is anyone who is or has been authorized access to a DoD information system whether a military member, a DoD civilian employee, or employee of another Federal agency or the private sector. Table 1 cites examples of insiders listed in the IPT tasking memorandum.

Employee	Network Connected User	IT Providers
Civilian or Military Contractors (e.g., outsourcing) Full-time, part-time, and temporary	Other Federal (Executive, Legislative) Contractors (e.g., acquisition systems) Colleges/universities Foreign partners, State & local, Other (EC/EDI)	Vendors and Suppliers (e.g., software development, maintenance)

Table 1. Insiders

The vast majority of insiders are hard working and dedicated to their respective professions, and they understand the importance of their work to the Nation. The vast majority of DoD insiders are firmly loyal to the United States. Insiders having security clearances know that they are obligated to protect the Nation's secrets and sensitive information.

This version of the report emphasizes the human insider, consistent with the tasking. However, this emphasis is problematic for information system security officials and the technology research community. Insider can mean 'system components' or 'computer software code' intended to carryout a malicious act. Appendix A includes many technology recommendations that address the non-human insider. These recommendations are only a starter set.

The problem of the outsider who gains information system access posing as an insider (an intruder) is outside the scope of the IPT. Nevertheless, the recommendations of the IPT mitigate or help to mitigate the malicious activity of anyone with insider access.

2.3 The Threat

Threat refers to the ability of an individual or organizational entity to exceed or abuse their authorized access to exploit, attack or otherwise misuse DoD information systems. The insider is different from an outsider because he or she is granted certain authorities and trust. Insiders have superior knowledge of asset value.

The insider has the capability to disrupt interconnected DoD information systems, to deny the use of information systems and data to other insiders, and to remove, alter or destroy information. Consequently, the insider who betrays the authorities, trust and privileges granted to them may be aided in their malicious activity by the very information systems upon which the Department depends. Aided by a team of highly sophisticated and well-resourced outsiders, the severity of insider malicious activity may be significantly amplified. However, regardless of motivation, the malicious insider (disgruntled employee, agent provocateur), can potentially reduce or compromise our military effectiveness, and place in jeopardy the lives of our military men and women.

The threat to Defense information has never been greater. As an example the environment for espionage is particularly conducive to the collection and sale of technical weapons system information. There is a growing inclination of those involved towards looking at such activities as business affairs rather than acts of national betrayal or treason. "Today, the greatest threat to these systems is from the insider, often an authorized user who performs unauthorized actions."[2] "Increasingly economic competition has redefined the context for espionage as nations link their national security to their economic security."[3] In addition to traditional Cold War era-type espionage, foreign visits to US facilities, joint ventures, conventions, and seminars, coupled with access to DoD information systems, may lead to successful espionage. The definition of an insider today can often be equated to these types of contacts. The recent espionage-related losses of nuclear weapons' design information is a classic example of the modern insider who has legitimate access to the data as well as legitimate access to government electronic communications' equipment. "US Government and cleared Defense contractor activities that were traditionally isolated from the general population are now increasingly vulnerable to exploitation."[4]

The Department acquires most of its information systems from vendors providing commercial off-the-shelf (COTS) products. Consequently, the Department has little or no knowledge of who developed the systems and, therefore, no measure of the trustworthiness, reliability or loyalties of those individuals. Contrariwise, individual developers of COTS products who have malicious intentions would have an extraordinarily difficult task to target a particular customer because COTS products tend to be produced in large quantities and shipped to customers as an activity that is independent of the individual developer. The developer with malicious intentions would have to deliver the same product to all customers while retaining the ability to isolate a particular customer for exploitation.

Detection of malicious code can be extraordinarily difficult. Historically, talented systems people (e.g., tiger teams and red teams) have been unable to convincingly demonstrate that an information system is secure; they are only able to demonstrate the many ways it is not. Over the years, information systems have become increasingly complex. The DoD has little or no influence over the development of COTS products. COTS systems are deployed with known errors, and it is still extraordinarily difficult to convincingly demonstrate that an information system is secure, and extraordinarily easy to demonstrate the many ways it is not. This is the risk information system security officials must attempt to manage.

The technology research community has several concerns, observations and questions about the insider threat not the least of which is the human-oriented definition of insider. Among their observations are:

- Malicious software code is a form of insider threat
- Insider misuse is hard to detect because it can operate at a higher semantic level than penetration by an outsider or an outsider attempting to masquerade as an insider
- Cyber outsiders can quickly attain many characteristics of an insider
- Not only must we reduce the risk of insider threat, we must prevent current malevolent insiders from hampering or subverting this process

More rigorous definitions of the insider are critical to structure research, and to set direction and guidance to allow research and development to progress efficiently.

Much attention is given the external security threat to information systems in the public and private sectors. This serious threat has existed for decades, however it has received greatly increased attention with the advent and expansive use of the Internet. The internal security threat has existed for centuries and is even more serious than the external security threat because the potential perpetrator of malicious activity is authorized access.

2.4 Threats to Classified and Unclassified Systems

The insider threat is to closed systems that process classified information and open systems that process unclassified information. Each is vulnerable to malicious insider action. Closed systems employ the same commercial-off-the-shelf software and hardware components used for information systems processing unclassified information – they contain the same fundamental vulnerabilities exploitable by the malicious insider. The basic difference between closed systems and open systems is the physical and technological wrapper around the closed system. The wrapper consists of physical security, unique communications protocols and stringent encryption that protects communications paths and prevents interception or disruption among network components.

Cleared insiders with malicious intent can cripple a closed system as effectively and more quickly than the external expert can cripple an open system. The insider has more time and knowledge of the system and its controls, and the insider is usually under no particular suspicion of malicious activity. The insider with access to a closed system processing classified information often has a network loaded with information that may be stored on removable media.

A DoDIG report[5] states, "AIS vulnerabilities are not limited to unclassified or sensitive unclassified systems. For example, of the 282 assessments [evaluations of security safeguards on operational, accredited information systems], 19 evaluated the safeguards on classified AISs. Of those 19 assessments, 15, or 79%, identified AIS vulnerabilities. Seven, or 37%, of the 19 assessments gained root access [system level access privileges including the ability to read all files, destroy information or applications, and deny access to authorized users, or the potential to connect to other AISs.]"

The DoDIG also notes that of 1,004 investigations associated with DoD information systems that may be criminal in nature, "164 (116 with internal intruders [insiders], 17 with external intruders, and 31 for which no intruder was identified) . . . of the 133 identified intruders, 116, or 87 percent, were either employees or others internal to the organization." Examples of these intrusions include:

- An employee who maliciously altered official medical records on the information system for an individual causing the hospital to cancel a scheduled appointment of surgery for that individual because the medical records could not be found
- An employee, by altering information system data, fraudulently routed shipments to a trucking company owned by a friend resulting in the government paying more than $500,000 for hauling freight illegally assigned by the employee
- A personnel clerk fraudulently entered data into the personnel database attempting to award herself a $500 performance award
- A DoD employee obtained an encrypted password file from a DoD classified network and decoded the password file at home, subsequently gaining unlimited access to the classified network, disruption on normal operations and the theft of DoD information resulting in a $4.78 million loss to the government.

It's very rare, but a small number of insiders for reasons of their own have betrayed the trust placed in them. Nevertheless, in a very large population of trusted insiders, when that small individual probability is multiplied by the size of the population, the probable number of actual malicious insiders a very large number in its own right. The potential damage a single malicious insider could cause has reached unprecedented levels. When malicious activity occurs, it is always taken seriously. DoD authorities take decisive action to minimize and assess the loss or damage, and enforce the law. No nation has successfully eliminated the insider threat. The challenge is to continuously assess the threat, reduce vulnerabilities to critical assets and seek new countermeasures.

2.5 Sources of Insider Problems

There are four basic sources of insider security problems.[6]

- Maliciousness[7] – that results in compromise or destruction of information, or disruption of services to other insiders
- Disdain of Security Practices –that results in compromise or destruction of information, or disruption of services to other insiders
  This problem results from willful:
  - public display of classified information; storage of classified material on unclassified media
  - unauthorized destruction of classified or unclassified data (e.g., For Official Use Only (FOUO) information, personnel or payroll data, other records)
  - lack of classified material protection outside of controlled facilities, to include unattended laptop computers containing classified materials
  - disruption of systems regardless of the sensitivity of the information they contain
- Carelessness – in the use of an information system and/or the protection of DoD information
  These problems are typically infractions of security policy and practices (e.g., breech of classified security requirements) for which the damage is usually determined to be minimal. While these insiders have the ability to exceed or abuse their authorized access to such resources, their motivation is not to exploit, attack or otherwise adversely affect DoD information systems.
- Ignorance – of security policy, security practices and information system use

Although the focus of the IPT is directed to mitigating malicious insider activity, it is worth noting that improvements in the security environment that may not be specifically directed at mitigating malicious

insider activity in fact mitigate that threat. For example, security improvements raise the security bar for everyone – those who:

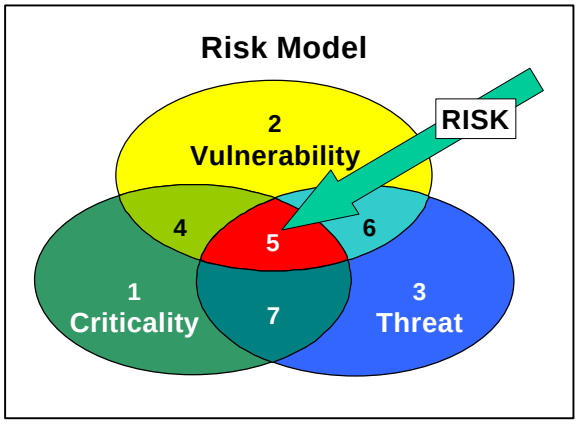
- Were unaware of good security practice or careless in their personal security practices become better aware of their responsibilities and are more attuned to the threat
- Disdain security practices may be less likely to do so
- May contemplate maliciousness may be deterred or will find perpetrating such activity more difficult or more risky

Sources of Information Systems Security/Usage Problems	Nature of the Threat	Probable Damage	Frequency *
Maliciousness (disgruntled employee or agent provocateur)	• Capability to Inflict Damage or Destroy, Compromise Intelligence • Enhances Potential for Outside Attacks • Deliberate Intent	Substantial	Unknown
Disdain of Security Practices	• Capability to Inflict Damage • Enhances Potential for Outside Attacks • Unintentional	Unknown	Unknown
Carelessness			
Ignorance			

Table 2. Threat – Damage Profile

2.6 Risk Management

Risk is the probability of loss or damage. Risk management is a function of three variables: criticality, vulnerability and threat. The first element is criticality; how important is this asset to the mission? The second element is vulnerability; in what ways can the asset be compromised, exploited, damaged or destroyed? The third element is threat; who intends to exploit a vulnerability, against what, and what capabilities do they possess to do so? Risk occurs at the intersection of criticality, vulnerability and threat. However, prudent management will focus on segments 4, 5 and 6. All DoD information, systems, programs, people, equipment and facilities reside within the DoD insider environment in this model.



Therefore, the strategy for mitigating the insider threat must:

- Consider the content and relationships among the risk model segments illustrated above
- Reduce the overlap area common to criticality, vulnerability and threat
- Require as a matter of prudence that some attention be given to reducing the number of vulnerabilities absolutely, and particularly those vulnerabilities that are known to be exploitable particularly should they become employed as part of a critical asset.

Note that threat, criticality, and vulnerability *dynamic*, not static, attributes. They must be re-evaluated often, especially during military operations or crisis situations.

Legend for numbered segments of risk model.
1 – Critical assets (information, systems, programs, people, equipment or facilities) for which there is no known vulnerability and no known threat exposure.
2 – Vulnerabilities in systems, programs, people, equipment or facilities that are not associated with critical assets and for which there is no known threat exposure.
3 – Threat environment for which there is no known threat to critical assets or access to vulnerabilities (or vulnerability information).
4 – Critical assets for which there are known vulnerabilities, but no known threat exposure.
5 – Critical assets for which there are known vulnerabilities and threat exposure.
6 – Threat has acquired specific knowledge and/or capability to exploit a vulnerability although not a critical asset vulnerability.
7 – Critical asset for which there are no known vulnerabilities, but there is exposure to a specific threat.

Part of risk management must also be a measurement and weighing of relative costs and benefits. Implementation of many of the recommendations in this report almost invariably places additional constraints on users or systems. Such constraints may well negatively impact productivity. A serious cost/benefit analysis must be done, weighing potential safety/security benefits against personal and organizational impacts on productivity and effectiveness. This analysis, however, is difficult; the "benefit of security can be somewhat intangible, as is the "cost" to personnel and organizations. Cost/benefit analysis of information security, as part of an overall risk management strategy, is an important topic that should be the focus of further research and attention.

2.7 Requirement and Strategy

The requirement is to:

- Define and enforce limits on overt access
  - Accountability for actions through reliable (non-refutable) records of actions
  - Review of recorded actions
- Detect unauthorized activity
- Deter
- Mitigate unauthorized activity
- Respond to unauthorized activity

Stated more broadly, the objective is to minimize the impact of the insider threat and to minimize the potential damage to DoD information or inflicted on DoD information and information systems by significantly reducing information system vulnerabilities to a wide range of misuse and abuse.

A wide range of choices is available to satisfy these requirements. Each choice brings with it a burden in human and fiscal resources and in implementation and maintenance time. For example, a number of different approaches, methods and tools can be employed to define and enforce limits on overt access, to review recorded actions, and to detect unauthorized activity. Other requirements must be much more precisely articulated before technologists will be able to offer credible solutions. For example, while certain behaviors are obviously unauthorized, the precise distinctions between what is ethical, conformant to policy or legal, and what is unauthorized is imprecise. To detect unauthorized activity the technologist first must have a precise and accepted definition of the term 'unauthorized' and its constituent behaviors. In the most rigorous context, solutions to some requirements are currently beyond the state-of the-art. Non-refutable records of actions and detection of certain unauthorized activity are examples. Research and development are needed to satisfactorily address these requirements. The risk model provides a way to begin to frame alternatives that can be applied commensurate with the criticality of assets, exploitable

vulnerabilities and specific threats – commensurate with the resources available and urgency to solve the problem.

Referring to the risk model, the Department must pursue the following strategy to minimize the impact of the insider threat. The Department must minimize the potential damage to DoD information or the damage inflicted on DoD information and information systems, too. These strategies are elements of an active security paradigm.

- Establish Criticality. Determine what assets are critical to the mission; declare what must be protected and to what extent; (DoD information and information systems) based on an analysis and assessment of what is required to accomplish the mission.
  [Risk Model segments 1, 4, 5 and 7.]
- Establish Trustworthiness. Seek to reduce the threat by establishing a high level of assurance in the trustworthiness of people, practices, systems and programs.
  [Risk Model segments 5, 6 and 7.]
- Strengthen Personnel Security and Management Practices. Develop and support a motivated, skilled and security-responsive workforce (deterrence).
  [Risk Model segments 1, 2, 4 and 7.]
- Protect Information Assets. Control asset sharing, isolate information and capabilities based on need-to-know (define and enforce limits on overt access, and deterrence), identify and reduce known information system vulnerabilities, and employ state-of-practice and new technology to enforce and support security policy.
  [Risk Model segments 1 and 7.]
- Detect Problems. Actively seek potential threats or problems (accountability for actions through reliable (non-refutable) records of actions and review of recorded action), whether isolated or correlated, that may result in anomalous or malicious activity (detection of unauthorized activity and deterrence).
  [Risk Model segments 3, 5, 6 and 7.]
- React/Respond. Correct suspected and actual unacceptable insider behavior using sound personnel, personnel security and system management practices (mitigation of unauthorized activity), and seek legal or other appropriate management remedies such as counseling to collection of forensic data to support possible prosecution (response to unauthorized activity and deterrence).
  [Risk Model segments 3, 5, 6 and 7.]

In addition to pursuing this strategy, the Department must also refine and update policies, procedures and practices to account for changes in operations attributable to changes in the military mission, the changing international security environment, and advances in technology.

(this page is intentionally blank)

3. Vigilance – A Template for Action

"Vigilance, Now" summarizes three areas for which the IPT believes the Departments can take immediate action to help mitigate the insider threat. "Vigilance – Looking Forward from a Strong Foundation" distills recommendations from the IPT working groups that provided numerous specific recommendations for mitigating the insider threat, and are scheduled or planned for future action.[8]

3.1 Vigilance, Now

Vigilance, Now includes actions in three areas: Awareness, exercised through personnel policies and deployed technology; Prevention, applied through existing, deployed technology; and Deterrence brought about by publicizing the consequences of misuse, abuse and malicious activity and the operational use of measures to detect those behaviors. Implementation of the recommendations in these action areas will "raise the security bar" across both classified and unclassified information systems environments.

The preponderance of IPT recommendations emphasizes the urgent need to "get back to basics" by supporting existing policy in personnel management, personnel security, information systems security even as these policies are being updated and strengthened. Practicing security basics is a prerequisite to mitigating the insider threat.

3.1.1 Increase Security Awareness/Reinforce Accountability

> A culture of information security is required throughout the Department of Defense. Policies and practices are at least as important as technical mechanisms. The current level of awareness is not commensurate to the threat. DoD basic information system security training for insiders has not received the attention it requires.[9]

Increased training and awareness are essential to inform insiders of their responsibilities, to reduce carelessness and to inform the potential malicious actor of the consequences of such behavior. DoD Components must assess their security training and awareness programs to determine whether and the extent to which these programs effectively sustain a security environment commensurate with their critical asset (especially information and information system) protection requirements. Effectiveness should be based in part on Component and Command security infraction and violation trends.

It is National policy that US Government departments and agencies develop and implement information system security training and awareness programs for national security systems. This policy is applicable to US Government departments and agencies, their employees, and contractors.[10] These policies and procedures are not being fully implemented today.

DoD must re-energize its efforts to communicate, clearly and frequently, information pertaining to information system threats, vulnerabilities, risks, and the responsibilities and accountability incumbent on the insiders to meet these challenges.

Security awareness, at a minimum, must consist of:

- *Basic Information Systems Security Awareness* – to address acceptable information system security behavior, general threats and vulnerabilities, a user-level protection regime and security events
- *Technology-focused Information Systems Security Awareness* – for privileged access insiders, and insiders having privileges to administer access controls and perform local administrative functions

The IPT presents two recommendations to improve Awareness.

Recommendation #3.1[11]: Communicate accountability and "acceptable use" policies and expectations, and enforce the established guidance.

Rationale: Senior DoD leadership has stated repeatedly that "information security must be a day-to-day responsibility." The power of information is multiplied through wise dissemination. Consequently, information security is harder and calls for greater sophistication on the part of all DoD insiders. The continuing need for information security accountability and awareness must be instilled in the entire workforce. Clear and persistent communication of security principles, goals and expectations of individual accountability is the first best step to mitigating the insider threat.

Recommendation #3.2: Implement IA/IT HR IPT[12] proposed recommendations for training, education, and certification of IA professionals.

Rationale: Enforcing training implementation and standardization provides for an alert and able workforce to deter and detect malicious insiders. The increased acuity to the threat by other DoD insiders, and the vulnerability and risk associated with discovery by peers is one the most effective and cost efficient approaches for preventing undecided individuals from committing espionage or sabotage.

3.1.2 Prevention – Protect Systems with Existing Methods and Tools

An effective defense requires at a minimum that already available protection capabilities be employed effectively.

Prevention begins with the insider – preventing individuals whose trustworthiness, reliability and loyalty cannot be satisfactorily assured from becoming or remaining an insider.

Recommendation #2.7: Employ maximum use of "data mining" once the Security Research Center completes its research, as detailed in Appendix A.

Rationale: Enables frequent or continuous monitoring of high risk (CAT1) insiders to detect anomalous behavior and thus provide warning of an increased security risk, and the possibility of a malicious insider.

Recommendation #2.10: Require contractors who use DoD information systems to meet the same requirements, contractually as government insiders regarding accountability, random computer audits, timely access changes, and password policy.

Rationale: Removes what otherwise could prove to be a weak link in the personnel security and management chain. This will also support PDD 63 by fostering the partnership between the public and private sectors. DoD should expect no less of its business partners processing DoD information then it does of the DoD workforce.

Recommendation #2.11: Require a written waiver approved by the head of the agency concerned before foreign nationals are permitted access to CAT1 IT functions.

Rationale: Limits performance of critical privileged access functions to cleared individuals.

The technological guardians and gatekeepers of the information revolution are access controls at the network, system, workstation entry points, directory and file level, public key encryption and controlled portals of entry – Intrusion Detection Systems (IDS),[13] Computer Misuse Detection Systems (CMDS), and internal firewalls.

Recommendation #4.7: Deploy a DoD Public Key Infrastructure (PKI).

Rationale: Helps to limit malicious insider unauthorized access to information; denies information reconnoitering and compromises.

Recommendation #5.1: Use firewalls internally to enforce compartmentation of information systems and assets.

Rationale: Limits malicious insider access only to those information domains or enclaves authorized.

Recommendation #5.2: Use existing technology under DoD IT operating systems (OS) software to disable writing to and booting from floppy disks or other removable media for critical and sensitive systems.

Rationale: Increases the work factor for the unauthorized transfer of large amounts of classified or sensitive information using large capacity removable media between systems processing at different classification levels, and of software or data that may contain malicious code or executables disguised in data.

Recommendation #5.3: Enforce mandatory and discretionary access control mechanisms to ensure that only users with the proper clearances and need-to-know are able to access classified or sensitive information.

Rationale: Limits malicious insider access to information assets based on a management judgment about the insiders need-to-know.

Recommendation #5.5: Apply virus scanners to centralized server computers and routers within an installation's local area network(s).

Rationale: Greatly reduces the likelihood of introducing known malicious code into the network.

Recommendation #5.7: Enforce established password policy and procedures, and require mandatory use of strong passwords, one-time passwords or encrypted passwords; bolster this requirement via the use of system features forcing strong password compliance.

Rationale: Strong passwords are a quick, low cost, readily available means to positively identify information system users.

Recommendation #5.9: Investigate the current availability of tools to enable uniform security-conscious configuration of application programs (such as Internet browsers, e-mail packages and office support software) within an installation, and monitoring of the configurations once installed.

Rationale: Limits or eliminates the introduction of unapproved applications, plug-ins and application configurations that could weaken information systems security.

3.1.3 Reinforce Deterrence

DoD requires real-time vigilance to deter, recognize, and respond to insider negligence or maliciousness. Two factors keep security issues and the insider threat at the forefront of the DoD insider routines. Feedback to DoD insiders on insider misuse, abuse or malicious activity issues, and publicity about on-going and up-coming defense-in-depth measures keep the attention of the insider. The publicized presence of capabilities to detect malicious activity and consequences imposed by the Department upon those who misuse, abuse or perpetrate malicious activity provides the greatest deterrent to malicious insider activity.

Three recommendations are presented to increase Deterrence.

Recommendation #4.1: Assure that more than one individual is authorized to access vital system operations and modifications, or perform duties of a security officer.

Rationale: Functional division of responsibilities limits the extent of certain privileged access and increases dependence on others to perform vital system operations – a checks and balances strategy.

Recommendation #6.1: Establish a mandatory program to randomly audit insider computer usage, the capability for intense monitoring of individual users, and for critical systems allow maintenance of a continuous map of selected users' activity.

Rationale: Aids discovery of the malicious insider. When formal responses to anomalies are apparent to all insiders, this program has a significant deterrent effect.

Recommendation #6.2: Develop tools for effective scanning and analysis of system and network audit logs to detect anomalous system and insider activity.

Rationale: Aids discovery of the malicious insider especially for privileged access insiders.

3.2 Vigilance – Looking Forward from a Strong Foundation

3.2.1 Underlying Principles

The Department must emphasize, first, practicing security basics:

- Reinforcing personal responsibility and accountability
- Developing personnel assurance commensurate with an insider's work and information access requirements
- Developing and maintaining good security practices across the workforce
- Using technology already deployed to raise the risk, cost and work factor of insiders who would perpetrate malicious actions, balanced by the need to make as much information as possible available to support mission accomplishment

The expectation, responsibility and authority to practice good security exist at every DoD organizational level, with every insider and with all DoD partners. None of these actions require new direction.

Strengthen the Policy Foundation. The IPT tasking is to recommend actions and policies that lead to establishing comprehensive security, acquisition and personnel practices to address the Insider Threat. Many of the IPT working group recommendations focus on specific functional policy. A comprehensive review of all existing policy is needed to determine its efficacy, and to diagnose and

repair flawed policy. Much additional work is needed to develop empirical information about the specific characteristics of the insider threat and its evolution (Recommendations #1.1 and 1.3). The Department must maintain empirical information on insider misuse, abuse and malicious activity to evaluate the character and significance of insider misuse, abuse and malicious activity. That baseline information is essential to assessing the efficacy of security-related policy and programs.

OSD/C3I must lead the Department in a thorough research of policy that impacts the insider. OSD/C3I must then lead the Department in updating and strengthening that body of policy where necessary, with the senior level commitment and resource support of the DoD Components.

Improve Deterrence, Visibly. The Department must use more effectively the methods and tools that improve deterrence. Notifying all insiders of the consequences suffered by insiders in recent cases and reminding insiders that there is no statute of limitations on espionage will help deter malicious activity.

3.2.2 Personnel Management

> Nothing can replace first rate management of subordinates, genuine concern for their well being, fairness, and recognition of personal warning signs for mitigating the insider threat.

Mitigating the insider threat begins with personnel selection and determination of suitability for service. The Department expects certain behaviors from insiders. Senior officials of personnel management processes must evaluate whether and how to measurably improve the methods of informing members of the workforce about:

- Expected standards of ethical behavior, particularly with regard to the custody and protection of DoD information and the use of DoD information systems
- The importance of protecting critical assets (information, systems, programs, people, equipment or facilities) regardless of the sensitivity of needed information access or the function performed
- Employee Assistance Programs for those who, through no fault of their own, encounter personal problems for which they are unable to cope without assistance

Similarly, managers and supervisors must live up to the expectation that they evaluate personnel effectiveness daily, develop the skills to recognize individuals who require special assistance and provide the avenue for them to acquire that assistance. For personnel performing in extraordinarily sensitive functions, supervisors should be required to develop subject matter knowledge in sufficient depth to understand the work processes performed by subordinates. This could provide limited workforce depth and a first line of detection for misuse, abuse or malicious activity.

3.2.3 Personnel Security

> Information warriors should have tattooed on the inside of their eyelids, "The enemy is already here."[14]

The presence of a malicious insider is a rare event, on an individual basis. However, the extremely large population of legitimate users (insiders), when multiplied by the individual probability, makes the probable number of actual malicious insiders a very large number in its own right.

DoD Personnel Security Strategy. The IPT personnel security working group recommendations focus on the functions performed by the insider having information system access, either to accomplish a DoD military mission or business function, or to ensure the integrity and proper operation of the information system. These functions require very different levels of technical expertise. Consequently, insiders who require access to system control functions, or control or influence information system performance perform an extraordinarily sensitive function. Therefore, the level of assurance in the trustworthiness, reliability and loyalty of these individuals should be commensurate with the sensitivity of the function they perform. Other occupations such as information operations, specialists in data correlation and those who are part of special access programs share this distinction of performing extraordinarily sensitive positions – often with less potential impact on the operation of the Department. The Department has many methods and tools to establish a level of assurance about individuals who perform in these sensitive functions. Every method and tool comes with a cost.

OSD/C3I must develop a Personnel Security Strategic Plan for determining the right mix of investigative, adjudicative and continuous monitoring methods needed to maintain an acceptable level of assurance in the trustworthiness, reliability and loyalty of the workforce (insiders). The plan must consider costs, including lower costs achieved by more discriminate use of investigative, adjudicative and continuous monitoring methods and tools, and higher costs attributable to more rigorous procedures and new operational requirements. The plan should seek new or refined personnel security models to better discriminate between the sensitivity of functions and the sensitivity of information, and to judiciously implement provisions for a strong deterrence to insider misuse, abuse or malicious actions against critical assets. The plan must resist the reflex to lay additional, oppressive administrative controls on the cleared population.

3.2.4 Security Education, Training and Awareness

The highest near term payoff to mitigate the insider threat is in security education, training and awareness.

OSD/C3I must, with the collaboration of the DoD Components, review all DoD sponsored security/counterintelligence-related education, training and awareness programs for opportunities to reinforce the need for heightened security awareness. OSD/C3I must foster the collaboration and coordination among what may be competing and overlapping education, training and awareness programs within security and counterintelligence communities, as well as within DoD elements performing these functions and the technology, such as advanced distributed learning. Finally, OSD/C3I must establish for the DoD and the supporting workforce, minimum education and training requirements for security.

3.2.5 Information Technology

> "Information technology is a weapon of mass destruction."[15]
>
> "Networks are weapon systems."[16]

Technology is an essential aid, not the solution to mitigating the insider threat. The Department must use effectively the technology already at its disposal to define and enforce limits on overt access, review audit records and deter unauthorized activity. DoD Components have authority through long-standing DoD policy[17] to implement an array of technology tools to mitigate the insider threat. While some

of these tools such as directory and file access permissions are administratively burdensome, DoD Component Designated Approving Authorities must weigh carefully the benefits and burdens of these methods, nevertheless.

Deploying new technologies such as the Public Key Infrastructure and Computer Misuse Detection Systems will further improve enforcement on overt access as resources permit.

The need for research and development in several areas is essential to keep pace with the increasing sophistication of the threat and the Department's dependence on information technology. Continuing, coordinated, collaborative research and development is needed improve authentication, prevention, detection and monitoring to cite a few research requirement areas. Research is needed to increase an adversary's risk, cost and work factor to perpetrate malicious actions. In addition, research must continue to develop technology to implement systems that can survive unstoppable attack and continue critical operations under fire.

The OSD/C3I/Defense-wide Information Assurance Program (DIAP) must continue play a key role by planning, coordinating, integrating and overseeing the Department's information assurance resources and investments. Further the DIAP must continue to provide for the research and development of IA technologies and techniques consistent with current and anticipated DoD mission needs and changes in information technologies. This broad mission must continue with the support and participation of the MILDEPs, Services and Defense Agencies. The DIAP must also leverage DoD, government, commercial and academic research, anticipate new technologies, develop synchronized IA solutions and leverage existing research coordination activities such as the INFOSEC Research Council.

(this page is intentionally blank)

Appendix A -- IPT Recommendations

Each recommendation contains two labels. One indicates the time frame in which the recommendation could be implemented.

"N" near term – six months or less
"M" mid term – six months to two years
"L" long term – lasting several years

The second label identifies the source of the recommendation as follows:

"P" IPT Personnel Management Working Group
"PS" IPT Personnel Security Working Group
"ET" IPT Education & Training Working Group
"T" IPT Technology Working Group
"S" National Security Telecommunications and Information Systems Security Committee (NSTISSC)
"N" National Research Council
"PPA" Political Psychology Associates, Inc.

Additional policies and initiatives may be warranted to address threat mitigation and vulnerability reduction, for example: further improvements in configuration management, installation of timely error corrections, and tool deployment across all CERT functions.

Some of the recommendations are not specific to the insider threat, but are included as part of a complete program required for implementing systems that are more robust in mitigating the insider, as well as other threats.

1. POLICY & STRATEGIC INITIATIVES

1.1 Develop and implement metrics tailored to the insider threat. (M) (T-44) (ET-1)

Discussion: Few metrics exist to evaluate insider threat mitigation. To make progress on mitigating the insider threat, the Department must measure the relative effectiveness and efficiencies of various approaches to preventing, detecting and thwarting unauthorized insider behavior. The Department must develop:

- Baseline data of the insider threat(s), vulnerabilities associated with critical information assets.
- Metrics to evaluate the effectiveness of intrusion and anomaly detection systems. Metrics are being developed and evaluated under DARPA contract. Much of that research may be directly applicable to insider attacks.
- Metrics to evaluate the effectiveness of insider threat training and awareness. This criterion will determine the ability of the training to change attitudes, improve knowledge, and increase skills.
- Metrics to evaluate the effectiveness of insider threat mitigation and vulnerability reduction programs.

By not pursuing this recommendation, DoD will continue to make, or not make, needed investment decisions based on intuition, anecdotal data and incorrect information. One expression describes the need for a baseline against which to measure progress and the need for measuring the correct indicators of progress or the intended outcome. "If you don't know where you are, any direction will do." Metrics tell you where you are.

Policy reference: Government Performance and Results Act (GPRA); DoDD 8000.1

Action: Recommendation requires new policy.

- OSD/C3I to draft proposed progress and outcome measures
- OSD/C3I to coordinate and issue metrics policy, program implementation and oversight guidance in this subject area; assign responsibilities and implement formal oversight actions

1.2 Conduct recurring workshops on technological approaches to mitigating the insider threat and reducing information system vulnerabilities. (N) (T-36)

Discussion: A workshop bringing together leading researchers and government officials can help assess existing relevant tools and techniques, and prioritize research and development activities required. The consequence of not implementing this recommendation is that time and effort may be expended by differing groups covering same or similar aspects of mitigating the insider threat thereby reducing the effectiveness and efficiency of the human, material and funding resources engaged. Key concepts and ideas developed by one group that could directly enhance the progress of another may not be fully exploited due to a lack of collaboration.

Policy reference: none

Action: OSD/C3I, in coordination with the INFOSEC Research Council members, will sponsor (periodic/semi-annual) invitational workshops.

1.3 Develop a database of insider events, characteristics, lessons learned and statistics. (M) (N-12) (N-13) (T-35) (T-46)

Discussion: The Department has no unified database of insider case studies, lessons learned, physiological profiles or statistics regarding the insider and insider misuse, abuse or malicious activity. This severely hampers understanding of the magnitude of the problem and development of solution strategies. The Computer Emergency Response Team community is developing vulnerability and incident databases for hacker related activity, but this is not focused on the insider problem. This database will be used to provide information and tools to policy-makers, personnel security, and security education personnel. Potential benefits from developing an insider event database cited in the context of various other IPT recommendations also focus on the need for improved detection, technical research priorities, and prevention through software engineering. Insider misuse, abuse and malicious activity is yet another manifestation of betrayal of trust behavior, comparable in many ways to police corruption, embezzlement, and espionage for which the Department must be alert to the appearance of patterns and situational foreground features seen in the study of espionage cases. The psychological profile should provide managers, security specialists and medical personnel a profile of the insider / computer abuser, which may become a useful tool to enable them to identify potential abusers before they cause serious damage.

At minimum, the following activities should be engaged for a unified insider database:

- Develop a framework for the information required
- Identify categories of problems
- Analyze differences/similarities of cases
- Provide managers, security specialists and medical personnel a physiological profile of the insider/computer abuser
  - This profile will assist in the development of questions for security investigations
  - This profile will define significant characteristic types of insider misuse
- Provide standardized material for security education, awareness and training
- Provide data for finer-grain access policies and differential access controls needed to help define what constitutes proper usage, thus facilitating the role of insider-misuse detection.
- Identify simple countermeasures available quickly
- Must be integrated with anomaly and misuse detection and network management in a trustworthy bi-directional manner
- Develop recommendations for technology solutions for future problems
- Identify useful current technology
- Prepare preliminary study results for workshop input

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: OSD/C3I to sponsor research into insider characterization and development of a characterization database of insider misuse, abuse and malicious activity.

1.4 Achieve defense-in-depth through use of multiple protection tools. (N) (T-42)

Discussion: Any protection tool may itself have flaws or weaknesses that can be exploited, or its capabilities may become known so that its protections can be avoided or bypassed. A layered defense should combine multiple, heterogeneous tools so that one product protects against the vulnerabilities of others. The concurrent employment of protection tools of different origins and the same fundamental purpose provides variability in the technical approach to protection. This increases the likelihood of success, but the cost as well. While diversity for this requirement is needed, strategies to employ diversity and maintain affordability must also be developed.

The consequence of not implementing this recommendation is that DoD information systems and networks would be denied the security benefits of multiple, independent protection tools that provide a layered defense. An enterprise wide susceptibility could prevail once the malicious insider has found an unobstructed path into the other system or network resources.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: OSD/C3I to examine the pros and cons of the defense-in-depth strategy, the impact on the DoD Joint Technical Architecture and interoperability standards goals, present IT acquisition strategy.

1.5 Assess technologies currently available for dealing with the insider problem. (N) (T-37)

Discussion: No coordinated activity currently exists to evaluate COTS and GOTS tools to address the insider. DoD should establish an activity to evaluate on a continuing basis the effectiveness of available COTS and GOTS security tools of all types.

The consequence of not implementing this recommendation is that DoD information systems may unnecessarily sustain a higher risk associated with the insider threat even when COTS and GOTS products may be available to mitigate that risk.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: OSD/C3I lead the establishment of this activity; include National Information Assurance Partnership (NIAP) and Defense-Wide Information Assurance Program (DIAP) personnel to work this issue.

1.6 Implement a new version of the Acquisition System Protection Program. (M) (J. Elliff)

Discussion: The current Acquisition System Protection Program (ASPP) is implemented inconsistently across DoD acquisition programs. Require program managers to develop protection plans by evaluating the threat to the information about their program and its vulnerability to compromise. The new version would be an Information Technology Acquisition Security Program that requires program managers to evaluate their vulnerability to sabotage/manipulation by surreptitious capabilities planted in commercially acquired components. If the vulnerability would jeopardize a critical Defense capability, additional security would be instituted.

Action on this recommendation is needed to provide an initial indication of criticality of procured systems and an identification of otherwise obscured system vulnerabilities.

Policy reference: DoD 5200.1-M, "Acquisition System Protection Program"

Action: OSD/C3I to work with the OUSD AT&L Acquisition Reform office to review program effectiveness and strengthen DoD policy to implement measurable improvement to the ASPP; review, and refine as necessary, requirement, guidance and program exit criteria for program manager implementation.

1.7 Direct the appropriate Defense agencies to accelerate the development of new tools for information systems security. (L) (S-5)

Discussion: The Department urgently needs a wide variety of new and improved information system security tools. Research and development investment must be redirected and/or new investment must be made. The threat from outsiders is evolving very quickly. Known corrections to information system vulnerabilities are corrected too slowly making those systems further vulnerable to malicious insiders. The Department's ability to develop or acquire trusted components and systems, to effectively manage system security, to monitor potentially malicious activity and to thwart actual malicious activity must mature more quickly. The pace of tool

research, development and deployment must be accelerated. A robust, aggressive and continuing research and development program is needed to counter the threats and reduce the vulnerabilities of information systems, for example,

- require R&D for configuration control
- systematic code verification to include vulnerability discovery in COTS and GOTS products
- fine-grained authorization
- tools for adaptive or active defense; accurate, rapid location of attackers
- security composition of secure systems and components to support ad hoc (e.g., coalition) activities
- better ways to configure and manage security features
- generation of useful security specification frrm programs
- more robust and secure architectures for networking requiring each packet to be traceable and certified authentic within a network fabric that denies transit to packets that cannot be authenticated, and automatic determination of classification from content

The Department must pursue develop and acquire new technologies to keep apace with the evolution of information technology and the Department's innovative uses of the technology. Unable to keep pace with tool research, development and deployment DoD systems faltering electronic protection and accountability measures will leave the gateways of access and unobserved operations open to insiders.

Policy reference: DoDD 5200.28, para. B-10, E-2-a, E-6-e; DoD 5200.1-R, 6-8 Alternative or Compensatory Control Measures

Action: OSD/C3I, with the collaboration of DDR&E and DIAP, review the Department's research and development investment portfolio for information system security with special attention to the insider issue; submit appropriate guidance for the incorporation into the Defense Planning Guidance; redirect, as necessary, current information system security R&D investments.

1.8 Develop solutions to the problem of "temporary insiders." (M) (T-43)

Discussion: Frequently groups of persons, such as coalition partners for a temporary operation, must be considered "insiders" for certain systems for a limited period. Special care and tools are needed during and after such operations to assure that access is appropriately limited during such operations, and removed when the operation is completed. Examples of the need for "temporary insiders" include coalitions formed for recent US military operations Desert Storm, Bosnia, Kosovo; contractors and others brought in to handle Y2K problems.

The consequence of not implementing this recommendation is that individuals no longer having the need to know and or no longer having authorization would be granted access to DoD information systems and information.

Policy reference: DoD 5200.1-R, 6-100, 6-201; DoD 5200.2-R

Action: OSD/C3I to lead the investigation of options, including but not limited to PKI, and develop recommendations to mitigate the problem of the "temporary insider."

1.9 Centralize coordination of activities addressing the insider problem. (N) (T-45)

Discussion: Activities that address the insider problem are currently distributed among a host of DoD organizations. One organization should assume responsibility to guide, coordinate and oversee the long-term efforts needed in this area. The activities must include operational, legal, policy, counterintelligence, law enforcement aspects of problem as well as activities to assess available technology, develop needed tools, identify research needs, etc..

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: The OSD/C3I Security and Information Operations office should serve as the coordination point to focus all activities related to mitigating the insider problem.

1.10 Perform research on identifying critical information, automatically. (M) (T-47)

Discussion: It is important to focus operational security measures on those items (information, aggregations of information, applications and hardware components) within an information system that are operationally sensitive, and/or are of high-value and critical to operations. Contemporary information systems contain a constantly shifting collection of gigabytes of data and information. It seems unlikely that static lists of critical files and processes will remain relevant. New concepts for OPSEC and advances in text mark-up languages should be key elements for research. This research recommendation addresses the question: Can procedures based on a set of business rules be developed by which critical information within a system is identified automatically?

Policy reference: none

Action: OSD/C3I should develop and sponsor an INFOSEC research program to address this recommendation.

2. PERSONNEL (MANAGEMENT AND SECURITY)

2.1 Enforce policy that requires immediate information system access removal for separated employees. (N) (P-3)

Discussion: Anecdotal evidence exists that computer system access is not always removed when employees separate from an organization. It is important that systems staff are informed immediately when user access requirements or authorizations change so updates to access privileges may be changed as close to the administrative change as possible. This is especially important for a staff member who is removed for cause – a person who may be disgruntled and wants retribution, but still retains system access.

The consequence of not implementing this recommendation is that individuals no longer having need-to-know or authorization will continue to have access to DoD information systems and information.

Policy reference: DoD 5200.1-R

Action:

- OSD/C3I to establish policy to include in the separation process the requirement for Human Resources offices to notify the Information System Security Officer (ISSO) of insider separation; include ISSO check-off on separation checklist.
- Direct ISSO remove insider from information system access authorization no later than COB of the insider's last duty day, unless otherwise required.

2.2 Create two distinct categories of information technology (IT) insider. (N) (PS-1)

Discussion: There is insufficient differentiation within the insider community to distinguish between those performing the functions of widely varying sensitivity. The potential to cause system wide damage to operating systems, system configurations, applications, stored data and if desired "cover ones' tracks" is directly related to system knowledge, system access and the capability to perform sensitive system functions. The current, proposed differentiation follows:

- Category 1 (CAT1): Positions involving privileged access to DoD IT systems with the capability to alter the intended operation or proper configuration of the system. (Includes the functions identified in the IA/IT HR IPT under System/Network Administration and Operations; Computer/Network Crime; Threat and Vulnerability Assessment; and Computer Emergency Response Teams, and Web security.)
- Category 2 (CAT2): Positions involving general access to DoD IT systems with read/write permissions, and whose incumbents can receive information from, input information to or modify information on, a system without a reliable human review.

Defining two categories of insiders captures the most sensitive functions performed by CAT1 insiders and correlates those functions to available investigative products employed by the Defense Security Service. More than two categories could prove confusing to the field and result in misapplication of the standards. (Note – An alternative under CAT2, due to the lack of a functional definition, would be to make this the "all other" category to include everyone with access to DoD information systems or networks.)

Policy reference: DoD 5200.1-R, 6-100, 6-201; 5200.2-R

Action:

- OSD/C3I will implement this policy change in a forthcoming revision to DoD 5200.2-R.
- OSD/C3I task IA community to draft and coordinate definition of functions performed by the CAT2 insider.
- OSD/C3I will cross-reference this policy in the Information Assurance directive or an update to DoDD 5200.28.
- OSD/C3I will investigate the use of PKI as a privilege management solution.

2.3 Establish personnel security vetting procedures commensurate with individuals' level of information system access. (N) (N-7)

Discussion: Insiders with privileged, root or super-user access are only required to undergo the same vetting procedures as other insiders even though the sensitivity of functions they perform and

the potential to access the most sensitive information contained in the system are much greater than those without such privileges. It is particularly important to focus on developing a strong security partnership with system administrators, ensuring that these individuals receive the best security awareness training available. Career development programs and industry accepted certification should be initiated consistent with the recommendations cited in the IA/IT HR IPT.

For DoD Components having authority to polygraph personnel, more frequent polygraphs are recommended for individuals having privileged access. Polygraphs could be supplemented by the creation of a special access program, including a security file review, for individuals with privileged access. For government offices without polygraph authority, additional emphasis should be given to background investigations.

The consequence of not implementing this recommendation is that insiders holding the positions with greatest privilege in DoD information systems will be held to an investigative standard inconsistent with the sensitivity of their position.

Policy reference: DoD 5200.1-R, 6-100, 6-201; DoD 5200.2-R

Action:

- OSD/C3I will develop resource requirements needed to implement this recommendation.
- OSD/C3I will incorporate the provisions recommended into revision to DoD 5200.2-R.
- OSD/C3I will work with the US Security Policy Board to develop updated adjudicative guidelines for "Misuse of Information Technology Systems."

2.4 Establish, as an investigative prerequisite, the requirement for a favorable Single Scope Background Investigation (SSBI) completed within the past five years for CAT1 insiders. (N) (PS-2)

Discussion: Clearances for CAT1 insiders are not vetted to the degree necessary to ensure sufficient trustworthiness to perform the most critical IT functions. The SSBI is the investigative prerequisite for TOP SECRET/SCI access and the most extensive investigation offered by DoD and should be used for CAT1 positions.

The consequence of not implementing this recommendation is that DoD information systems will be vulnerable to access by individuals placed in critical positions without sufficient trustworthiness to hold those positions. Appropriate candidates will be delayed in placement, investment in time, knowledge and indoctrination will be wasted and information systems security will suffer from placement of an untrustworthy insider.

Policy reference: DoD 5200.1-R, 6-100, 6-201; DoD 5200.2-R

Action:

- OSD/C3I will develop resource requirements needed to implement this recommendation.
- OSD/C3I will implement this policy change in a forthcoming revision to DoD 5200.2-R.
- OSD/C3I will work with DoD Comptroller to ensure that sufficient resources will be available for DSS and the DoD Components to assume the Cat 1 investigative workload.

2.5 Establish, as the investigative prerequisite, the requirement for a National Agency Check, Local Agency Checks and Credit Check associated with access to

SECRET or CONFIDENTIAL access (or NACI for civilian personnel by OPM) for CAT2 insiders. (N) (PS-3)

Discussion: Investigative standards for CAT2 insiders are not vetted to the degree necessary to ensure sufficient trustworthiness to perform many sensitive IT functions. The current investigative standard in DoD 5200.2-R for Cat 2 is a National Agency Check for military and contractor personnel and a National Agency Check plus Written Inquiries (NACI) for civilian employees. The new National Agency Check with Local Agency Check (NACLC) and ANACI (for civilians) provide sufficient additional investigative coverage for the sensitivity of the duties for the Cat 2 IT insider.

The consequence of not implementing this recommendation is that DoD information systems and information will be exposed to individuals lacking a sufficient level of trustworthiness for critical positions relating to the use and operation of information systems equipment.

Policy reference: DoD 5200.1-R, 6-100, 6-201; DoD 5200.2-R

Action:

- OSD/C3I will develop resource requirements needed to implement this recommendation.
- OSD/C3I will implement this policy change in a forthcoming revision to DoD 5200.2-R.
- OSD/C3I will work with DoD Comptroller to ensure sufficient funding is identified to perform this function, including contractor personnel under the DSS fee for service program.

2.6 Conduct minimum periodic reinvestigations (PRs) at a 5-year interval for Cat 1 IT positions and a 10-year interval CAT2 IT positions. (N) (PS-7)

Discussion: Many individuals that will fall into proposed Cat I and Cat 2 IT positions have not had and are not required to under go PRs. Category 1 positions require privileged access to DoD IT. The IA/IT HR IPT identifies these positions under System/Network Administration and Operations; Computer/Network Crime; Threat and Vulnerability Assessment; Computer Emergency Response Teams and Web security. Category 2 positions require general access to a DoD IT system.

The consequence of not implementing this recommendation is that minimum safe standards for identifying possible inappropriate or malicious behavior or changes in personnel characteristics detrimental to information systems security and security of DoD information will not be met, placing those systems and information at increased risk.

Policy reference: DoD 5200.1-R, 6-100, 6-200; DoD 5200.2-R

Action: OSD/C3I will to publish, pending satisfactory completion of the Security Research Center's pilot program, the baseline PR requirements in a revision to DoD 5200.2-R with sufficient flexibility to implement the aperiodic data mining PR.

2.7 Employ maximum use of "data mining" to enable continual online review of personnel security information. (M) (PS-7)

Discussion: Most cleared insiders committing espionage or other malicious activity do so between traditional PRs. This indicates that five years is too long a period of time to wait for a Periodic Reinvestigation (PR) for very sensitive positions. The Security Research Center is conducting an

evaluation of the feasibility and costs of monitoring security risk indicators between PRs. IT security will be better served if a "continual on-line review" of personnel security information is applied as opposed to waiting five years before initiating required reinvestigations. Data mining could be a largely automated operation that would be less expensive and applied to a larger population than the traditional PR. If the data mining PR turned up potentially significant issues, then a full-fledged field investigation could be initiated.

The consequence of not implementing this recommendation is that important indications of a possibly malicious insider could go unheeded during the intervening years between formal periodic reinvestigations.

Policy reference: DoD 5200.1-R, 6-100, 6-201; DoD 5200.2-R

Action: OSD/C3I will to publish, pending satisfactory completion of the Security Research Center's pilot program, the baseline PR requirements in a revision to DoD 5200.2-R with sufficient flexibility to implement the aperiodic data mining PR.

2.8 Include appropriate questions in the Single Scope Background Investigation (SSBI) to address on-line behavior for CAT1 and CAT2 insiders. (N) (PS-12) [PPA-1]

Discussion: Interview questions have not yet taken into account the ease of communicating with foreign nationals and aberrant behavior over the Internet that may indicate unsuitability for a position of trust. Background screening procedures designed to detect the risk factors associated with insider violations should include questions relating to on-line contacts, computer addiction, previous hacking behavior, computer violations, unauthorized access and fraud.

The consequence of not implementing this recommendation is that a new indicator of potential personnel security problem will not be employed to screen individuals who may be inappropriate for a trusted position.

Policy reference: DoD 5200.1-R, 6-100, 6-201; DoD 5200.2-R

Action: OSD/C3I will task DSS to develop and implement questions pertaining to subject's on-line behavior.

2.9 Mandate completion of minimum requirements prior to permitting a CAT1 insider to assume assigned duties. (N) (PS-8)

Discussion: Verification of trustworthiness for personnel assigned CAT1 duties is not consistent with the interim clearance procedure for DoD personnel security program. This is consistent with the interim clearance procedures for the DoD personnel security program and incorporates a sufficiently stringent but flexible regime to balance mission requirements with the need to put trustworthy personnel to work expeditiously. Minimum requirements should be:

- A favorable check of the Defense Central and Investigations Index (DCII) has been conducted
- A favorable review of the Standard Forms - 85 Supplemental Questionnaire for Selected Positions (SF-85PS) has been accomplished
- A favorable review of available local records has been conducted
- The SSBI/PR has been initiated to DSS

While DoD activities are authorized to issue interim clearances, industry is not. DoD Components and contractors could electronically forward the necessary information to the CAF for an expeditious determination and issuance of an interim Letter of Trustworthiness.

The consequence of not implementing this recommendation is that DoD information systems and information will be placed at increased risk of compromise or denial of service by access of individuals lacking verification of an appropriate level of trustworthiness for such access.

Policy reference: DoD 5200.1-R 6-100, 6-201; DoD 5200.2-R

Action: OSD/C3I will include appropriate policy change in impending revision of DoD 5200.2-R and coordinate with appropriate DoD and industry groups.

2.10 Require contractors who use DoD information systems to meet the same requirements, contractually, as government insiders regarding accountability, random computer audits, timely access changes, and password policy. (N) (P-5)

Discussion: The DoD contractor workforce that is authorized access to DoD information systems is not subject to the same INFOSEC policy and procedural requirements as Government insiders. This DoD contractor workforce increasingly uses or has access to the Department's information systems. DoD contracts that require or include authorized contractor access to DoD IT needs to require compliance with DoD INFOSEC policies and procedures. Additionally, the costs that will be imposed on the contractor in relation to the insider threat, especially if any of the investigative (or adjudicative) missions becomes a contract cost.

This workforce must be subject to the same policies as the DoD employees. Thousands of DoD contracts will have to be reviewed and changed to comply.

The consequence of not implementing this recommendation is that the benefits of DoD personnel security and information assurance efforts will be compromised by allowing individuals not meeting DoD employee minimum standards access that could otherwise be denied in accordance with current DoD employee access policies.

Policy reference: DoD 5200.1-R 6-100, 6-201; DoD 5200.2-R

Action:

- OSD/C3I will incorporate into the DoDD 8500.xx, "Information Assurance," the requirement that contractor access to DoD information systems will satisfy the same requirements as required for DoD military members and civilian employees.
- OSD/C3I will task the AT&L/Procurement Policy to provide guidance to Contracting Officers to ensure these requirements are included in affected contracts.
- AT&L will provide guidance to ensure that all DoD IT contracts are revised to reflect the insider threat policies.

2.11 Require a written waiver approved by the head of the agency concerned before foreign nationals are permitted access to CAT1 IT functions. (N) (PS-4)

Discussion: Non-US. citizens may not be granted a security clearance. However, many foreign nationals may be under contract to perform privileged access functions such as system or network administrator for DoD information systems. No one is aware of the magnitude of foreign national involvement. This recommendation is consistent with existing requirements of DoDD 5200.28 as well as the provisions of the personnel security program in DoD 5200.2-R and E.O. 12968. Foreign national contractor personnel may already be employed in CAT1 functions in support of DoD contracts. These persons will either have to be grandfathered in following a risk assessment and waiver, or moved out of their CAT1 duties.

The consequence of not implementing this recommendation is that DoD information systems and information will be placed at increased risk of compromise or denial of service by virtue of foreign nationals having CAT1 access and lacking the appropriate level of trustworthiness for such access.

Policy reference: DoD 5200.1-R, 6-100, 6-201; DoD 5200.2-R

Action:

- OSD/C3I will implement this policy change in a forthcoming revision to DoD 5200.2-R; ensure consistency with DoDD 5200.28.
- OSD/C3I will determine the magnitude of CAT1 foreign nationals; issue appropriate policy.

3. TRAINING & AWARENESS

3.1 Communicate accountability and "acceptable use" policies and expectations, and enforce the established guidance. (N) (P-1) (T-41)

Discussion: Private sector "best practices" require employees to sign security agreements before being given access to information systems. Additionally, the private sector in the IT industry includes compliance with security rules as one of the elements of their employee performance evaluations. There is no similar policy for the DoD. The Department must hold insiders accountable for fulfilling their information systems security responsibilities. Accountability is reinforced by an institutional environment of continuous security awareness and a reputation for timely, consistent, and fair discipline.

Civilian and military policies, the Uniform Code of Military Justice (UCMJ) and the Manual for Courts Martial all have punitive measures that are currently used for computer security offenses.

The Department and its Components should establish clear, consistent "acceptable use" policy and guidelines on secure and appropriate use of IT systems. These policies and guidelines should be presented to users in a simple and clear form (e.g., not using legal jargon) on a regular basis (e.g., not less than twice a year).

Policy reference: DoD 5200.1-R, chap 1, 1-101

Action: OSD/C3I will prepare action to convene C3I, OSD General Counsel, and Personnel & Readiness representatives to examine existing policy and practices regarding acceptable use of DoD

information systems, and determine how existing methods of communicating "acceptable use" and accountability may be improved.

3.2 Implement proposed recommendations for training, education, and certification of IA professionals. (N) (ET-2) (N-8) (T-38)

Discussion: The referenced IPT recommendations[18] contain extensive research on the training requirements for the CAT1 and CAT2 insider, particularly those with "privileged access." These reports recommend a number of human resources initiatives to dramatically improve the management and training of DoD personnel assigned these critical IA functions. Recommendations include the implementation of an extensive renewable mandatory certification and training process for this segment of the workforce, the development of an Advanced Distributed Learning (ADL) system to deliver and update this IA training and manage the certification administration, and completion of background investigations.

Implementation of these and other recommendations in the referenced reports substantially reduces the current threat to the Department's warfighting capability by ensuring that our first line of defense in information warfare is fully trained in the skills required to protect the integrity and availability of both critical operational information as well as the supporting infrastructure. Training will ensure that they possess the knowledge and skills required to maintain continuous, predictable configuration control and systems security, a working knowledge of current IT security countermeasures, and appropriate expertise in external and internal threats (unauthorized behavior) against IT systems.

Policy reference: DoD 5200.1-R, chap 9

Action: DepSecDef should direct the implementation of the recommendations of the referenced reports.

3.3 Establish mandatory minimum standards for security education, awareness and training programs related to the insider threat. (N) (ET-1)

Discussion: The content of security training and awareness programs is not consistent across the Department. There is no prescribed minimum course curriculum or set of baseline training and awareness requirements. With few exceptions, information technology awareness training is not documented. All authorized users must be trained and made aware of information systems security issues and requirements. The Military Departments and DoD Agencies must consistently emphasize the importance to our warfighting capability of information systems security.

Effective training and awareness courses, when recognized by the authorized user as an important priority, can mitigate the threat of careless or thoughtless actions that put our systems at great risk. The Department must establish a practice of "Orientation before Participation." Training must be successfully completed before the individual is granted access to the system or network. Individuals who fail or do not complete the annual training will have their system and/or network access temporarily removed until the refresher training is successfully completed.

Measurement criterion must be created for determining the effectiveness of the insider threat training. This criterion would determine the ability of the training to change attitudes, improve knowledge, or increase skills.

Policy reference: DoD 5200.1-R, chap 9

Action:

- OSD/C3I will reiterate the requirement to implement exiting policy and procedures for initial information technology security training for insiders.
- OSD/C3I will enforce existing policy and procedures that require annual, recurring security and awareness training for all insiders.
- OSD/C3I will request the DoD Inspector General to establish a special interest item to review compliance with the above actions during audits and inspections.

3.4 Consolidate, into a single electronic source, basic information assurance training material, customized or enhanced to address the insider threat and made accessible to all authorized users, security managers and training professionals. (M) (ET-3)

Discussion: Each Military Department and DoD Agency has an independent security training and awareness function and activity. This structure lacks a consolidated electronic source of basic information assurance training material. Such a consolidated database would make it possible to provide uniform and cost-effective training and education on the insider threat. The Defense community would benefit from a capacity to amass and share insider threat training and awareness information. The IPT recognizes the need for agency and department specific training criteria. However, independent efforts in a well-defined discipline can be unnecessarily duplicative and produce an inconsistent quality of training. To eliminate these inefficiencies the Department must standardize insider threat training and awareness programs across agency and service boundaries. Uniformity in training would ensure quality and foster a common understanding and awareness in dealing with the insider threat.

Policy reference: DoD 5200.1-R, chap 9

Action:

- OSD/C3I will task DISA to lead a Department-wide program and to create a single source database as the preferred resource for insider threat security training and awareness.
- OSD/C3I will direct Military Departments and DoD Agencies to post insider threat incidents, incident responses, lessons learned and best practices into the consolidated database.
- OSD/C3I will direct DISA to develop and post in the consolidated database a baseline-training module on the Insider Threat to ensure consistency of training.

3.5 Develop a threat awareness package for all users of DoD information systems. (M) (S. DeVito)

Discussion: The DoD workforce does not yet appreciate the threat to DoD information systems or the importance of their responsibility to contribute personally to the protection of those systems and the information. Users should be apprised of the threats, foreign and domestic, to DoD computer networks. A threat awareness package should be developed that focuses on genuine events and developments that elucidate real problems with information stored and manipulated on computers and transmitted over the public switched networks. Supervisors should be made aware of the management and psychological issues that impact the modern workforce. A team of law

psychologists could produce threat awareness packages tailored for supervisors at various echelons. In addition, this team could develop a threat package for the massive number of individual users that could educate them to the realities of knowledge protection.

The consequence of not implementing this recommendation is that the vast number of DoD employees will "remain in the dark" about issues, characteristics and threats posed by those individuals who may contemplate or plan malicious activity.

Policy reference: DoD 5200.1-R, chap 9

Action:

- OSD/C3I will task DSS to develop a plan for implementation of this recommendation; identify specific requirements and methods in collaboration with other DoD Components, and resources for sustaining a current threat awareness program.
- OSD/C3I DIAP, in collaboration with the Military Departments and DoD Agencies, will establish training effectiveness measures. These measures must be related to "insider" incidents caused by carelessness, ignorance or negligence on the part of the authorized user.

4. DETERRENCE

4.1 Assure that more than one individual is authorized to access vital system operations and modifications, or perform duties of a security officer. (M) (T-39)

Discussion: System and network administrators hold critical positions in maintaining operational and security effectiveness of DoD systems and networks. From an insider threat perspective, these positions are high risk. A system of checks and balances or a two-person rule would reduce the likelihood of introducing inadvertent errors into DoD systems and reduce the potential for malicious activity. Specific emphasis should be made on separation of duties between security and operations functions of an organization. Security personnel must have both the authority and systems access to provide oversight of security-related functions in any network.For very critical systems, software tools should be developed to require "two-person" cooperation and coordination.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: OSD/C3I will examine the security benefits (referencing the Nuclear Weapons Personnel Reliability Program) balanced by the skill and manpower requirements of the recommendation; draft policy memo, as appropriate, for Department-wide implementation.

4.2 Mandate use of "warning banners" or other on-line messages that serve to raise the awareness of insiders to the need for secure and appropriate system usage, and that highlight recent observed misuse and its consequences. (N) (T-2)

Discussion: Insiders become habituated to routine banners presented during the log-on procedure and often no longer make any cognitive connection with either concept or detail of the information presented. Traditional, "legalistic," fixed notices are routinely ignored or even generate frustration,

particularly for sophisticated users. A changing notice that highlights recent observed misuse and its consequences would be more effective. For example, publish the percentage of bad passwords found and the number of notices of misuse behavior sent to management.

Implementation of banner and on-line messages viewed by users at random times, advertising information systems security accountability and practices will be a quick and low cost method for "raising the bar" of awareness over the entire insider community. These notices would contain the following types of information: individuals use of system may be monitored, ensure use of this system and related storage media are confined to authorized areas only, questions regarding authorization or that of any other insider or reporting any unauthorized access or use should be directed to the Information Systems Security Officer.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action:

- OSD/C3I will review, and revise as appropriate, DoD policy for security awareness banners and other on-line security messages.
- OSD/C3I will issue guidance, provide strategies and assign functional responsibility for administering a consistent, Department-wide bannering and on-line security messaging program.

4.3 Ensure that management invokes minor sanctions for low level infractions of the stated security policy, in order to demonstrate the organization's commitment to the policy. (N) (T-1)

Discussion: A security policy that is not backed up by enforcement is soon ignored. Enforcement measures can have a significant deterrence effect. Sanctions for low level infractions have the triple purpose of punishing malicious behavior, reminding users that the security policy is enforced and deterring users from such behaviors.

The consequence of not implementing this recommendation is that DoD employees who disregard fundamental information system security principles will continue to do so with impunity; overall information systems security will be lowered. Motivation for understanding and adhering to policies, procedures and best practices for mitigating the insider threat will be diluted.

Policy reference: DoD 5200.1-R, chap 1, 1-501 (1)

Action: OSD/C3I, in collaboration with OSD/Personnel and Readiness, will determine whether and what additional requirements and/or guidance is necessary to implement this recommendation, including the value of appropriate language for insertion into the mandatory security performance element of military and civilian supervisors.

4.4 Develop and use procedures for random reviews of system administrator logs by another System Administrator, chosen randomly and anonymously. (N) (T-40)

Discussion: Their knowledge of system operation and 'super' user privileges needed to do their job make system and network administrators the greatest potential threat to DoD information systems. System administrators have the greatest knowledge of system operations and control over system

facilities. As such, they have the greatest capability to perform malicious actions. Special attention must be paid to monitoring of System Administrators, especially in critical systems.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: OSD/C3I to draft and coordinate policy memo.

4.5 Create technology providing a tamper-proof audit trail recording the actions of individuals authorized access to sensitive data and networks. (M) (T-3) (N-10)

Discussion: Tamper-proof audit trails are vital in later forensic analysis after events occur, and in prosecuting malicious and destructive actions. Tamper-proof audit trails are analogous to airplane "black box" recorders that provide a robust record of recent events in a cockpit for later analysis. Such recording might be hardware-implemented (e.g., writing on a write-once CD-ROM) or software-based with strong encryption, digital signature, and other controls to prevent tampering and allow the detection of any modifications. Several research issues must be addressed including determination of what information to retain, and for how long given the growing volume and bandwidth of information being transmitted within networks. These decisions will involve tough cost/benefit tradeoffs.

Such audit trails must stand up to legal scrutiny.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action:

- OSD/C3I/DIAP will coordinate the research issues of this recommendation and propose an appropriate research program to implement the intent of this recommendation.
- OSD/C3I to work with the DoD Office of the General Counsel to establish the legal requirements and limitations for tamper-proof audit trails.

4.6 Consider means by which changes can be traced in all documents generated within an organization, by simple and tamper-proof modifications to existing widely used office automation programs. (M) (T-4)

Discussion: An audit trail is needed for a document generated and transmitted within an organization, including the inception, modification, and transmission of the document. Several possible approaches should be researched, such as digital signatures within larger plans for a DoD Public Key Infrastructure. Research approaches for such traceability include "watermarking" and "fingerprinting" of documents. (See also recommendation 5.12, below, for further discussion of traceability within a larger, integrated security architecture.)

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: OSD/C3I/DIAP will coordinate the research issues of this recommendation and propose an appropriate research program to implement the intent of this recommendation.

4.7 Deploy a DoD Public Key Infrastructure (PKI). (M) (T-5)

Discussion: Certificate and public key technology represents a substantial benefit in dealing with the insider threat. Continue the implementation of PKI technology for all DoD Components.

Through its management of certificates, the DoD PKI provides technical solutions that can facilitate mitigation of the Insider Threat problem. The DoD PKI provides life cycle management of identity and encryption certificates and can bind privilege information of individuals to these certificates. Applications enabled to use these PKI certificates use identity certificates for controlling access to DoD networks and digitally signing of information to verify both the identities of end users and the integrity of the information. The DoD PKI also uses encryption certificates for confidentiality of data as appropriate.

The DoD PKI Program Management Office, in recognizing the magnitude of its role and the impact on the future of DoD information systems, should incorporate plans and procedures to mitigate the insider threat throughout the development, deployment, and operational phases of the program. Furthermore, it is imperative that the DoD PKI Program Management Office develops technologies with specific attention paid to the ability of PKI to help users deal with insider threat problems.

The ASD(C3I) recently assigned NSA with Program Management responsibility for the Department's efforts to implement a Public Key Infrastructure (PKI).

Policy reference: DepSecDef memo, "DoD Public Key Infrastructure (PKI)", May 06, 1999

Action: Memorandums tasking the DoD PKI PMO should include a statement reflecting the need to pay particular attention to addressing the insider problem in establishing a DoD PKI system. DoD Components shall pay particular attention to addressing the Insider problem when enabling their applications to be interoperable with the DoD PKI.

4.8 Individual Defense organizations should review and possibly restrict access to private (non-DoD) Internet Service Providers (ISPs) from within internal DoD systems. (N) (T-6)

Discussion: The indiscriminate use of personal ISPs for work purposes – e.g., to host work web pages or forwarding e-mail – should be reviewed and possibly restricted. Each DoD Component must consider the risks posed by such use to their environment and take appropriate steps to limit access where necessary. Use of private ISPs from within an internal DoD system creates an unnecessary risk for all other interconnected systems.

Policy reference: DoD 5200.28 (Encl. 5) Network considerations; DoD 5200.40, IT Security Certification and Accreditation Process

Action: OSD/C3I will issue policy memo requiring DoD Components to implement recommendation.

5. PROTECTION

5.1 Use firewalls internally to enforce compartmentation of information systems and assets. (N) (T-19)

Discussion: Firewalls may not be in use to control insider access to what are otherwise Intranets. Most firewalls are focused upon the outside attacker and are not being used effectively to limit local users. DoD Components should available firewall systems internally to appropriately limit the activities of users as they now exit the internal network, and to segregate – when possible – internal networks.

The consequence of not implementing this recommendation is that the time proven strategy of enforcing need-to-know restrictions and appropriate insider isolation through the compartmenting of information will not be fully employed within the virtual work place.

Policy reference: none

Action: OSD/C3I will draft policy to implement this recommendation Department-wide.

5.2 Use existing technology under DoD IT operating systems (OS) to disable writing to and booting from floppy disks or other removable media (e.g. off line storage hard disks) for critical and sensitive systems. (N) (T-10)

Discussion: Permitting information to move from system to system via "sneaker net" presents a real danger to critical and sensitive systems regardless of the rationale for the information movement. In practice the action of inappropriate "sneaker net" transfers can degrade 'Dedicated' or 'System high' security mode to a multilevel security mode. Wherever operationally and technically possible, access to removable media should be electronically disabled. Physical removal or locking of such devices may be appropriate. One or more controlled portals of entry can be established allowing users to surrender portable material to information systems security personnel for processing and entry into or exit from the information systems architecture.

The consequence of not implementing this recommendation is that inappropriate use of portable electromagnetic media will continue to contribute to the unauthorized transfer across of information DoD information systems.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: OSD/C3I convene a workshop of DoD Components to evaluate Component policy and procedures for control of removable media, review the pros and cons of extant technology based solutions; OSD/C3I will draft policy for Department-wide implementation.

5.3 Enforce mandatory and discretionary access control mechanisms to ensure that only a user with the proper clearances and need-to-know is able to access classified or sensitive information. (N) (N-4)

Discussion: Mandatory and discretionary access control mechanisms available in current DoD information systems are not consistently used. Systems that process classified and sensitive

information need to enforce mandatory and discretionary access control mechanisms to insure that only users with the proper clearances and need-to-know are able to access this data. DoD managers at all levels must work with ISSOs to periodically review access permissions.

Access control mechanisms need to be deployed not only at network boundaries but also within the client-server computing environment (to limit unauthorized insider access). The use of such mechanisms require that appropriate data labels (or other mechanisms) be used to identify the access control ground rules – for individual files, messages, databases, etc. Until viable mandatory access control mechanisms become widely available, systems processing different levels of information must remain isolated and each must enforce discretionary access controls.

Techniques that should be investigated as potentially useful access control mechanisms include:

- Biometrics – the use of automated methods of identifying or recognizing persons based on physiological or behavioral characteristics, such as fingerprints, speech, facial characteristics, iris or retina patterns, handwritten signatures or hand geometry. Biometrics provides a more robust, more reliable method of authentication than many current methods, although care must be taken in their installation and use to prevent "spoofing" (e.g., substituting previously recorded signals in place of a live verification.
- Proximity badges – a badge worn by a user that can be sensed by his or her workstation. The workstation might be set to lock up if an authorized user's presence is not sensed. The convergence of the DoD Common Access Card that will include a PKI certificate and the configuration of DoD computers to work only when the smart card is in the computer smart card reader shows promise.
- Access control software – that locks a system after an idle period, requiring a password to reinstate the display. A significant insider vulnerability is the unattended, yet logged-in, workstation. If used, care must be taken that such systems are tamperproof. The workstation idle period before locking should also be carefully adjusted to balance security concerns with possible reduction of user productivity caused by this measure.
- Frequent or periodic re-authentication during a user access session – to aid in preventing an insider from masquerading as another legitimate user. One possible approach to continuous or periodic authentication would be to require the presence of a personal "token" (e.g., smart card, or similar device) during a session, although this is not a fool-proof mechanism.
- Time-of-day/day-of-week controls – in which various permissions and user access attributes are based upon time of day or day of week. These may aid in denying unauthorized access to IS systems during unusual and unsupervised hours. Again, use of this mechanism must be balanced against the most effective and efficient use of information systems resources.

Policy reference: DoDD 5200.28

Action: OSD/C3I will develop DoD-wide guidance for DoD Components to employ access control mechanisms available with COTS products, as a minimum, including the DoD PKI.

5.4 Configure virus scanners to test all floppy diskettes and other removable media when introduced; the scanners should not be capable of being disabled by the end user. (N) (T-8)

Discussion: Floppy disks and other removable media are an important "port of entry" for malicious code and a convenient medium to remove classified and sensitive files from secured areas. Floppy

diskettes should be scanned for viruses and other problem software when first introduced into a computer or network. All DoD Components should download, install and use virus-scanning software for which the Department has enterprise licenses.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: OSD/C3I will draft policy for Department-wide implementation.

5.5 Apply virus scanners to centralized server computers and routers within an installation's local area network(s). (N) (T-7)

Discussion: Virus checking is currently often not performed on internal severs and routers within DoD internal networks, only on external firewalls and portals. Scan e-mail and its attachments with virus checkers at the router or mail server. It is an effective, centrally managed method of protecting the system from viruses. This centralized checking should be performed at system boundaries and portals. All sites should install a firewall or filtering router to screen common types of attacks. All sites should routinely access an authoritative source of information on network and system attacks (e.g., CERT advisories) to stay on top of new vulnerabilities and types of attack.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: OSD/C3I will draft policy for Department-wide implementation.

5.6 Deploy media or file encryptors that transparently encrypt sensitive data, data recovery mechanisms to ensure that encrypted data can be recovered (M) (T-11) (N-9)

Discussion: Unprotected data stored on user workstations and data servers is vulnerable to a number of insider attacks. Files and media that are encrypted make inappropriate access to their information much more difficult for the insider. File encryption refers to actions taken to individual files. Media encryption applies such actions to entire media, such as a hard drive for back up disks. The use of encryption might not be accepted unless it is relatively transparent in operation. The use of this technology may need to be studied further. Also, the "strength" of the encryption technology used must be evaluated and considered; a false sense of security resulting from use of a weak product may be harmful. The evaluation of software encryption products may take long enough for this to be considered a medium-term recommendation.

DoD Components should be encouraged to widely deploy media or file encryptors that transparently encrypt sensitive data. Particular attention needs to be paid to the mechanisms that generate and store the key encryption keys used for this purpose to insure that they are resistant to insider attacks. In addition, data recovery mechanisms need to be used to insure that appropriate authorities can recover the encrypted data in the event of a lost or damaged token or other failure condition.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: OSD/C3I/DIAP will coordinate the research issues of this recommendation and propose an appropriate research program to implement the intent of this recommendation.

5.7 Enforce established password policy and procedures, and require mandatory use of strong passwords, one-time passwords or encrypted passwords; bolster this requirement via the use of system features forcing strong password compliance. (N) (N-5) (P-4) (T-9)

Discussion: Current documentation for all OSD components requires use of strong passwords in protection of both classified and unclassified OSD information systems. A research initiative is needed to establish the security and economic impact of replacing passwords with strong authentication mechanisms that require the use of tokens or biometrics (for user login) and cryptographic authentication (for network interactions).

Poorly chosen passwords can be corrected in very short order through the use of already-available technology. The system can force the selection of "strong " passwords. The system can force password changes as frequently as desired. The system can control the number of unsuccessful log-in attempts. And the system can determine the vulnerability of the chosen password and take corrective action. This is a very low solution that can be implemented within a very short time frame based on existing technology in the Department's inventory.

Require use of strong passwords and frequent changing of passwords (e.g., as described in the DoD Password Management Guideline), regular system administrator use of password crackers, and use of built-in system features to control password age and composition. Wherever possible, eliminate the use of long term passwords and adopt one-time password technology. For particularly sensitive situations, biometric-based authentication should be used to verify the user's access to a terminal, laptop, or workstation.

Policy reference: DoDD 5200.28

Action:

- OSD/C3I will draft policy for Department-wide implementation to establish a mandatory baseline password policy covering systems both classified and unclassified. This policy will establish minimum requirements for:
  - Passwords; configuring servers to require the use of "strong" passwords, at least 8 characters in length with at least three of the following four features: an uppercase letter, a lowercase letter, a number, or a special character
  - Maximum Password Duration; password lifetime requirements and automatic expiration features
  - Personal Password Policy; password protection and password sharing
  - Use of encryption
  - Controls on log-in attempt rates
  - Audit trails
  - Password vulnerability checks and follow-up

- OSD/C3I will, through appropriate channels, direct CINCs, Services and Agencies to educate organizational supervisors at all levels of the risks of password sharing and the technical

alternatives available to get the job done; ensure that systems staffs are trained on how to provide these alternatives.

5.8 Mandate periodic use of existing tools for vulnerability assessment on systems and networks. (N) (T-20)

Discussion: Many DoD system administrators do not currently use existing software toolkits to probe for known vulnerabilities of systems and networks. System administrators should use these tools to evaluate their own system vulnerabilities before malevolent parties do so.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: OSD/C3I will task DISA to evaluate tools and develop guidelines for their use, locally.

5.9 Investigate the current availability of tools to enable uniform security-conscious configuration of application programs (such as Internet browsers, e-mail packages and office support software) within an installation, and monitoring of the configurations once installed. (N) (S-4) (T-16)

Discussion: Many vulnerabilities are caused by inappropriate or incorrect system configuration. System/network administrators, in coordination with the ISSO, should develop a "safe" initial configuration for every system type and application under his or her control. This safe configuration should then be used as the distribution copy for software installations within the site. It may be necessary to develop, or sponsor the development of, software tools to aid in such configuration control for major Defense installations.

DoD-wide use of proper configuration management would be an important step toward upgrading the security of DoD information systems to the level of best practices in the private sector. Network management tools can continuously monitor the operational configuration of a network and all of its component machines, alerting the administrator when variances from known and safe configurations are detected. Furthermore, they can also be used to authenticate all computer-to-computer communication; thus all communications carried in the network can be authenticated rather than just those origination from outside a security perimeter.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: OSD/C3I will task DISA to investigate the availability of tools to support this recommendation; OSD/C3I/DIAP will coordinate research requirements identified by DISA and propose an appropriate research program to implement the intent of this recommendation.

5.10 Conduct independent vulnerability assessments. (N) (N-16)

Discussion: The Department lacks funding to support independent, unscheduled vulnerability assessments. All systems have technical and operational vulnerabilities; a continuing search for those weaknesses is essential. Independent and unscheduled vulnerability assessments, from the broad system level assessments to penetration testing to red teaming, are a good way to periodically check the security health of information systems. These assessments need to encompass all aspects

of insider threats and vulnerabilities. The DoD needs to support and fund a program to conduct frequent, unannounced penetration testing of DoD information system architecture.

The consequence of not implementing this recommendation is that DoD information systems state of security will not be independently evaluated, areas of vulnerability may well go undetected for long periods of time, unnecessarily increasing risks to information systems and information to insider attacks. Reliance exclusively on personnel directly involved with specific systems to monitor and self police those systems will dangerously increase risks not only with regard to an insider deliberately masking weak conjuration management but also individual personnel who may not be as astute in the application of system security features being the only evaluator of the "health" of a particular system.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: OSD/C3I will propose Defense policy to implement this recommendation.

5.11 Mandate use of tools for effective destruction of information/media waste products so that they are unavailable to insiders (or outsiders). (N) (T-18)

Discussion: Discarded floppy disks, printouts and the like may contain sensitive unclassified information, yet be treated casually within a controlled environment available to the insider. Insiders have easy access to wastebaskets and other casual repositories of discarded materials before they are properly disposed of. Destruction devices such as shredders or magnetizers should be easily accessible to users, and their use mandated for sensitive materials at the time they are discarded.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: OSD/C3I will draft policy to implement this recommendation Department-wide.

5.12 Continue research on developing a system security architecture sensitive to the demands of the insider threat. (M/L) (T-48)

Discussion: System security architectures, in general, are inadequate. When available, they do not adequately address the unique problems associated with the insider threat. A security architecture, at minimum, should be comprised of:

- Authentication components – the ability to uniquely identify entities in a system and between systems with a high level of assurance
- Access control components – permitting access control with fine detail such as per file, per transaction, per packet, and so on
- System integrity components – that continuously check system integrity, to prevent violations of integrity caused by such malevolent software available today as Back Orifice 2000 (BO2K), "Root Kit," and the Melissa virus

- A bi-directional trusted path to the security system – the availability of which is a fundamental component of a secure architecture and involves authentication in both directions of a transaction
- Attribution components – allowing a system to attribute specific actions to specific users. Approaches to this problem include watermarking (placing subtle or invisible marks in objects that attribute those objects' origin), and fingerprinting (watermarking that identifies where the object has been). Such attribution mechanisms must be hardened against possible insider misuse

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: OSD/C3I should continue sponsorship of the IA Working Group adding appropriate additional emphasis to mitigation of threats from the malicious insider.

6. DETECTION

6.1 Establish a mandatory program to randomly audit insider computer usage, the capability for intense monitoring of individual users, and for critical systems allow maintenance of a continuous map of selected users' activity. (M) (P-2) (T-27)

Discussion: DoD has not visibly demonstrated that it audits insider computer use. Deterrence may reduce the risk of some deliberate malicious acts. Tracking the number of abuses discovered and acted on, and examining trends will provide a measure of effectiveness. One of the private sector's "best practices" is to establish a well-publicized program of randomly auditing employee computer usage. The private sector ranks this practice very high as a deterrent to improper and malicious behavior.

DoD Components should establish a program for random auditing of insider activity. While the detailed and continuous auditing of all individuals may well be cost prohibitive with current technology, aperiodic (i.e., random) detailed auditing of users could be effective and affordable. DoD should develop requirements for random auditing of user activity. Requirements for the program should include definitions of what will be audited, how data will be analyzed, how results will be reported and to whom, and average frequency of audit. At individual DoD Component sites, the results of audits as well as the average frequency of audit should be publicized. This program should have the following characteristics:

- Automate the audit to the fullest extent possible
- Publicize the program among all users on a recurring basis
- Notify each insider audited in a manner similar to the notification cards left on desks by security staff checks for improperly secured classified material
- Clear guidelines of what will be audited and how results will be reported and to whom

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action:

- OSD/C3I/DIAP will coordinate the research issues of this recommendation and propose an appropriate research program to implement the intent of this recommendation.
- OSD/C3I to work with DoD OGC to develop a mandatory requirement for all DoD Components to implement a program to randomly audit computer usage to identify improper, suspicious or malicious insider activity.

6.2 Develop tools for effective scanning and analysis of system and network audit logs to detect anomalous system and insider activity. (M) (T-24)

Discussion: It does little good to collect elaborate audit trails and logs if insufficient tools are available to locate anomalies and misuse patterns recorded as raw data within those logs. It is necessary to scrutinize the online activities of individuals with root privilege and/or broad "need-to-know" access. This will be costly and labor intensive but the real threat of audits can do much to deter the insider problem. Auditing can establish normal computer use profiles, and thereby enable the detection of abnormal patterns. The development of additional audit/profiling tools, such as an icon that would alert the user to ongoing monitoring, could assist this effort. Additionally, auditing the use of printers and other removable media would disclose the removal of large quantities of data. More attention must be paid to effective log scanning tools and analysis tools that minimize “false positives” while finding important security-relevant events.

The consequence of not implementing this recommendation is that anomalous system activities of DoD insiders will go unnoticed, vital indications that can be gleaned from exiting audit traits will go unprocessed, the most important aspects of an established audit trail will go unrealized, detection and accountability. Devoid of the ability to transform audit data into information systems security intelligence the auditing security will become a virtual paper tiger.

Policy reference: OMB Circular No. A-130, Appendix III, “Security of Federal Automated Information Resources”

Action: OSD/C3I/DIAP will coordinate the research issues of this recommendation and propose an appropriate research program to implement the intent of this recommendation.

6.3 Configure and deploy existing intrusion detection systems to monitor the activity of insiders. (N) (T-21) (N-11)

Discussion: Intrusion detection systems are typically not currently tuned and configured to detect malicious insider activity. Enormous amounts of energy have been expended using intrusion detection systems to detect attacks from “the outside;” yet little or no attention has been directed to applying this technology to the insider problem. Intrusion detection systems should be positioned at multiple levels within an information system (e.g. local workstation, host levels). Special attention should be given to detecting anomalous insider activity, activity associated with not only entry into and within a system, but also egress from the system. For example, a compendium of “signatures” of high-risk insider misuse is needed in order to configure signature-based systems to detect system misuse.

The consequence of not implementing this recommendation is that important indications of unauthorized insider behavior within DoD information systems will go unnoticed and not acted

upon, increasing insider vulnerability and cracking a powerful cycle of security, protection, detection, restoration and response.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: OSD/C3I/DIAP will coordinate the research issues of this recommendation and propose an appropriate research program to implement the intent of this recommendation.

6.4 Implement use of network mapping tools to detect any alterations in the configuration of a network. (N) (T-22)

Discussion: All system administrators must maintain an accurate and current "mapping" of their network, yet existing tools are often mot used for this purpose. System and network administrators must have an accurate and real-time understanding of the configuration of the system and network for which they are responsible. Inexpensive tools exist that can provide system and network administrators with valuable information about their network.

The consequence of not implementing this recommendation is that system and network administrators will remain unaware of current system and network configuration status or possible unauthorized modifications made by DoD insiders. The insider may permanently or "periodically" weaken the system, exploit that weakness, then return the system configuration to the original state.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: OSD/C3I/DIAP will coordinate the research issues of this recommendation and propose an appropriate research program to implement the intent of this recommendation.

6.5 Develop and use software tools that check file and access permissions within system and flag potential problem areas. (N/M) (T-23)

Discussion: Some system controls make it too easy for a user to give read or write permission to "everyone" – perhaps as a temporary expedient, but then such lax permissions linger unnoticed within the system. Proper file access permissions on files are highly dependent on the importance of the data involved, the user's preference for sharing files with people with access to the network, the type of file involved, and the type of access needed to have the files be useful to users (read, write, and or execute).

Complicating this issue is that file permissions are often set too loosely and not with the intention of protecting the information involved. Unfortunately, for a large networking file system, the system administrator does not and should not (due to need to know and other security issues) have knowledge of the content and the need to share files with other users. There must be communication between the system administrator and the owner of the files to assure that file permissions are set up correctly. The system administrator may be able to tell what files "seem" to be set with lax permissions, but they do not know if they actually are without checking with the owner of the files.

A project leader who owns and maintains files in a network file system may be required, to use a two-part tool. The first part is a visualization and file permission tool letting the owner of a file structure see what file permissions are set, and provides the owner a list of files that might be set too

high. The goal is to make file security and permissions much easier to view, change, and give owners an idea of the vulnerability of their files. Owners then have the opportunity to correct breaches in security and specify the importance of their files and the frequency of their use so that a misuse detection tool can monitor them. The second part is a misuse detection tool that monitors file access based upon user specified importance of the files, the frequency and type of access, and the inherent vulnerability of the file permissions set.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action:

- OSD/C3I/DIAP to task DISA to investigate the availability of COTS products to simplify the administration of network, system and file permission maintenance.
- OSD/C3I/DIAP will coordinate the research issues of this recommendation and propose an appropriate research program to implement the intent of this recommendation.

6.6 Perform research and development on the concept of "honeypots" specifically tailored to attract insiders. (M) (T-28)

Discussion: "Honeypots" are not widely deployed on DoD information systems either as a deterrent to malicious activity or to collect evidence of malicious activity. An established technique for determining the intentions and sophistication of malicious actors within an information system is to deploy files of information that appear attractive and important. These "honeypot" files, configured to signal when they are accessed, give an early indication of possibly malicious intentions or action, provide early warning of insiders whose probes and actions are outside the bounds of expected and normal behavior. More study, including legal consultation, must be done on appropriate and inappropriate uses of this technique, and guidelines established for its proper use.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: OSD/C3I/DIAP will coordinate the research issues of this recommendation and propose an appropriate research program to implement the intent of this recommendation.

6.7 Develop better tools to detect the introduction of malicious "mobile code." (M) (T-30)

Discussion: Recently, a new insider threat has emerged with Internet connectivity to every desktop: mobile code (such as Java applets, software agents, ActiveX controls, various forms of Web scripts, and e-mail attachments). Unlike the traditional insider threat, introduction of mobile code does not require malicious intent on the part of insiders; they can unknowingly download, install, and execute mobile code that can compromise system assets with as much damage as an ill-intentioned insider. Many forms of mobile code download and execute transparently to the end user – that is, the end user may not have realized that he or she downloaded someone else's programs and executed them on their machine with their privileges. Those downloaded programs might open trapdoors, read e-mail folders, mail documents or even sabotage systems.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: OSD/C3I/DIAP will coordinate the research issues of this recommendation and propose an appropriate research program to implement the intent of this recommendation.

6.8 Create a comprehensive list of system and user behavior attributes that can be monitored to establish normal and abnormal patterns to enable anomaly and misuse detection. (M) (T-25)

Discussion: There is no comprehensive list of system and user behavior attributes available to baseline normal activity patterns and thereby enhance recognition of anomalous user activity. More research attention is needed to develop the set of best system and user behavior attributes that should be monitored, both to establish normal patterns and to find abnormal patterns.

Misuse detection systems often rely on "signatures" of activity that signal potential system misuse. A compendium of system and user behavior attributes will enable the construction of such "signatures" of malicious insider behavior, each signature being a collection of one or more values of such attributes. Statistical-based systems can also be used to identify normal vs. abnormal behavior, and discover malicious insider activity.

The consequence of not implementing this recommendation is that system administrators and information system security managers will be over overwhelmed by the shear volume of user characteristics data; without an established inventory of behavior attributes and patterns grounded in counterintelligence experience and stored to allow for rapid automatic analysis and monitoring, the desired product of actionable intelligence about abnormal patterns of system recourses and user activities will be unattainable.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: Working with the counterintelligence community, OSD/C3I/DIAP will coordinate the research issues of this recommendation and propose an appropriate research program to implement the intent of this recommendation.

6.9 Establish a broad-based, long-term research program in anomaly and misuse detection addressing specifically the insider threat. (L) (T-29)

Discussion: Overall, there many important gaps in our basic understanding of anomaly and misuse detection. This severely limits ability of the Department to deal with malicious insider threats. Much more research and development work remains to be done to fill in these gaps. The following items should be included in and give direction to such a long-term research program:

- The commonalties between insider misuse and outsider misuse, with respect to threats, methods, exploitation, detection techniques, and response approaches, and take advantage of those commonalties where possible, resorting to different but compatible approaches where commonality is not immediately evident. The possibly significant differences between insiders and outsiders, such as the relative lack of need for "reconnaissance" activities by an insider, especially a system administrator must be better understood.
- Significant effort must be devoted to defining characteristic types of insider misuse.
- Finer-grain access policies and differential access controls are needed to help define what constitutes proper usage, thus facilitating the role of insider-misuse detection.

- Much greater effort needs to be devoted to detecting unknown modes of misuse, rather than just focusing so heavily on detecting known attacks. The existing statistical paradigms must be pursued and refined. However, new paradigms must also be considered.
- The community at large needs to address hierarchical and distributed correlation of results aggregated across different sensors, different application platforms, and different analytic tools. The correlation must seek to identify common patterns and intent, such as those resulting from coordinated distributed attacks.
- Anomaly and misuse detection must be integrated with network management in a trustworthy bi-directional manner.
- Much better software engineering is needed to make the analysis systems interoperable, robust, evolvable, and extensible in their application domains to monitoring other attributes such as reliability, fault-tolerance thresholds, survivability, performance, etc.

Anomaly and misuse detection platforms must themselves be:

- tamper-proofed to hinder integrity attacks on the platforms, alterations of evidence (either by wrongdoers to cover their tracks, or by law enforcement in attempting to contrive evidence)
- spoof-proofed to hinder bogus denial-of-service attacks on the platforms
- robust to provide stability of the analysis platforms.

Investigation of extrinsic individual characteristics such as psychological behavior might be included in profiling user activities.

Over time, such a long-term research program will enhance the ability of the Department to detect anomalies and misuse in the operation of its computer systems, thereby increasing its capabilities to deal with malicious insider threats.

The consequence of not implementing this recommendation is that discernible patterns and indications of insider malicious activity will not be developed, severely hampering efforts to automate the scrutiny of appropriate and inappropriate DoD information system user activities. Although the artificial intelligence applications may not be on-line today to effectively and efficiently identify precursors to malicious insider activity; without the body of material resulting from the formal study and research of insider anomalies will delay bringing important misuse detection tools on-line once appropriate AI applications are available. DoD will be faced with employing antiquated methods to scan an ever-increasing volume of user data on systems that continue to proliferate through out the department.

Policy reference: OMB Circular No. A-130, Appendix III, “Security of Federal Automated Information Resources”

Action: OSD/C3I/DIAP will coordinate the research issues of this recommendation and propose an appropriate research program to implement the intent of this recommendation..

7. REACTION/RESPONSE

7.1 Create tools for a rapid and effective audit of a host computer system, to detect any anomalies in its programs and files. (M) (T-31)

Discussion: Tools for the rapid and effective audit for anomalies are immature. Support tools are needed to help a system administrator take a rapid and effective "audit" of a system, to help in determining whether anomalous and/or malevolent actions have been taken within this system. Once an anomaly is suspected in the programs and files of a host computer system, there must be a way for a system administrator to quickly ascertain whether such anomalies exist, and what is their form and content. Such tools do not exist at present in a satisfactory form.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: OSD/C3I/DIAP will coordinate the research issues of this recommendation and propose an appropriate research program to implement the intent of this recommendation.

7.2 Develop capabilities to do forensic analysis of intrusions. (M) (T-32)

Discussion: A "toolkit" of software programs and aids must be developed to allow a complete forensic analysis of an event in a manner that will withstand scrutiny in legal proceedings. Capabilities to perform after event / action forensic analysis will provide DoD personnel with the resources to gain valuable lessons learned from insider IS incidents resulting from both careless and malicious insider events. Information obtained from this "toolkit" will be directly applicable to several other proposed initiatives relative to migration of the insider threat e.g. centralized database of insider attributes, insider threat awareness package, and general information systems security awareness and training material.

The consequence of not implementing this recommendation is that DoD insiders caught engaging in unauthorized activities may well escape administrative sanctions due to mishandling of the evidence of those activities, weakening deterrence within the DoD. Without post event analysis many important lessons learned will go untapped as resource material for insider related research on insider profiles, techniques, database correlation and development of insider threat mitigation tools and procedures.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: Working with the counterintelligence community, OSD/C3I/DIAP will coordinate the research issues of this recommendation and propose an appropriate research program to implement the intent of this recommendation.

7.3 Conduct research on means of reacting to suspected insider malicious activity. (M) (T-33)

Discussion: Inadequate tools and techniques currently exist to react when insider malicious activity is suspected. It should be possible to track an insider's activities carefully, thoroughly and

inconspicuously, as a reaction to indicators of suspicious activity. These tools should be available in the medium-term, and not dependent on the outcome of a long-term R&D program. An insider may access, download, copy, damage, or remove large volumes of information from an information system quickly. Reaction tools are needed to aid system administrators and security personnel to quickly assess potential problems, apply tracking and surveillance tools, conduct damage control as necessary, and so on. If warning signs are unclear or ambiguous, it may be necessary to track a user's activities surreptitiously for an extended period. These tools must be usable by system administrators without requiring extensive training and expertise.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: Working with the counterintelligence community, OSD/C3I/DIAP will coordinate the research issues of this recommendation and propose an appropriate research program to implement the intent of this recommendation.

7.4 Conduct a long-range research program on reaction to insider threats. (L) (T-34)

Discussion: A longer-term research program is needed to address the insider threat at a more fundamental level, in addition to the specific near- and medium-term recommendations for reacting to an insider incident. Among the capabilities required for a robust and flexible reaction capability tailored to the malicious insider problem are these:

- **A pre-positioned global network of reaction systems** capable of: 1) creating traffic among sets of information systems in order to degrade malicious insider capability covertly; 2) sensing changing network topologies and conditions to enable the reaction systems to control information flows within the infrastructure; and 3) analyzing the situation relative to coordinated timing data for information flows at various network nodes.
- **Deception systems** capable of: 1) taking over ongoing communication sessions between identified parties in a manner that avoids noticeable alterations in system behavior; 2) simulating the network environment in which the normal system operates, in order to convince an attacker that the simulated environment is the real one; and 3) replacing internal services on the fly without noticeable impact on user behavior or performance.
- **Analysis and response "stations"** capable of: 1) gathering, fusing, and analyzing data received from distributed reaction and deception stations within the network; 2) controlling reaction and deception systems in order to mitigate consequences of an attack while avoiding detection by the attacker; and 3) analyzing current and future situations in order to anticipate the need for action and pre-positioning of capabilities allowing rapid reaction to future events.
- **Real-time and post-mortem forensic systems** capable of: 1) gathering and storage of historical and real-time information from all available data sources, and fusing the information to allow for analysis of events over time, and by type, across systems and infrastructure components; 2) generation of paths of entry and location of sources and intermediaries used by the attacker, based on the available audit information; and 3) correlation of information from diverse sources of audit information that is partially redundant, and analysis to determine whether the redundant information tends to confirm or refute hypothesized sequences of events.

Policy reference: OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

Action: Working with the counterintelligence community, OSD/C3I/DIAP will coordinate the research issues of this recommendation and propose an appropriate research program to implement the intent of this recommendation.

Appendix B -- Policy References

DoDD 5200.1, “DoD Information Security Program,” December 13, 1996

DoDD 5200.2, “DoD Personnel Security Program,” April 9, 1999

DoDD 5200.28, “Security Requirements for Automated Information Systems (AISs)”, March 21, 1988

DoD 5200.1-M, “Acquisition System Protection Program,” March 1994

DoD 5200.1-R, “Information Security Program,” January 1997

DoD 5200.2-R, “Personnel Security Program,” January 1987

DoD 5200.40, “IT Security Certification and Accreditation Process”

OMB Circular No. A-130, Appendix III, “Security of Federal Automated Information Resources”

DepSecDef memo, “DoD Public Key Infrastructure (PKI)”, May 06, 1999

(this page is intentionally blank)

Appendix C -- Glossary

accountability – Process allowing auditing of information system activities to be traced to a source that may then be held responsible.

anomaly detection system – Detector configured to identify behavior that deviates from normal system usage.

authentication – Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

banner – Information displayed by the information system that sets parameters for system or data use.

biometrics – Automated methods of authenticating or verifying an individual based upon a physical or behavioral characteristic.

countermeasure – Action, device, procedure, technique, or other measure that reduces or eliminates one or more vulnerabilities

data aggregation – The compilation of unclassified individual data systems and data elements resulting in the totality of the information being classified.

data mining – The analysis of data for relationships that have not previously been discovered

digital signature – Cryptographic process used to assure message originator authenticity, integrity, and nonrepudiation. Same as electronic signature.

discretionary access control – Means of restricting access to objects based on the identity and need-to-know of users and/or groups to which the object belongs. Controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (directly or indirectly) to any other subject. See mandatory access control.

firewall – System designed to defend against unauthorized access to or from a private network. Firewalls can be implemented in hardware and software, or a combination of both.

granularity – Relative fineness to which an access control mechanism can be adjusted.

inadvertent disclosure – Accidental exposure of information to a person not authorized access.

information assurance (IA) – information operations that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

information assurance red team – Independent and focused threat-based effort by an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to improve the security posture of information systems.

information operations (IO) – Actions taken to affect adversary information and information systems while defending one’s own information and information systems.

information security (INFOSEC) – the system of policies, procedures, and requirements established under the authority of E.O. 12958 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

information system (IS) – The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.

information systems security – Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

information systems security manager (ISSM) – Principal advisor on computer security matters.

information systems security officer (ISSO) – Person responsible to the designated approving authority for ensuring the security of an information system throughout its life cycle, from design through disposal.

integrity – Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Internet protocol -- (IP) Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.

malicious code – Software or firmware capable of performing an unauthorized function on an IS.

mandatory access control – Means of restricting access to objects based on the (MAC) sensitivity of the information contained in the objects and the formal authorization (i.e., clearance, formal access approvals, and need-to-know) of subjects to access information of such sensitivity. See discretionary access control.

misuse detection system – Detector configured to identify behavior that matches a know attack scenario.

national security system – Any telecommunications or information system operated by the United States Government, the function, operation, or use of which: 1. involves intelligence activities; 2. involves cryptologic activities related to national security; 3. involves command and control of military forces; 4. involves equipment that is an integral part of a weapon or weapon system; or 5. is critical to the direct fulfillment of military or intelligence missions and does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (Title 40 U.S.C. Section 1452, Information Technology Management Reform Act of 1996.)

private key – Encryption methodology in which the encryptor and decryptor use the same key, which must be kept secret.

privileged access – Explicitly authorized access of a specific user, process, or computer to a computer resource(s).

public key infrastructure (PKI) – Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software.

risk management 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.

sensitive information – Information, the loss, misuse, or unauthorized access to or modification of, which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national Defense or foreign policy. (Systems that are not national security systems but contain sensitive information are to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L.100-235).)

system administrator (SA) – Individual responsible for the installation and maintenance of an information system, providing effective IS utilization, adequate security parameters, and sound implementation of established INFOSEC policy and procedures.

time-dependent password – Password that is valid only at a certain time of day or during a specified interval of time.

two-person control – Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements.

two-person integrity (TPI) – System of storage and handling designed to prohibit individual access to certain COMSEC keying material by requiring the presence of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.

(this page is intentionally blank)

Appendix D -- Abbreviations and Acronyms

ASD(AT&L)	Assistant Secretary of Defense (Acquisition & Technology)
ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
ADL	Advanced Distributed Learning
AI	Administrative Instruction
AIS	Automated Information System
ANACI	Access national Agency Check with Written Inquiries
ASPP	Acquisition Systems Protection Program
C3I/S&IO	Command, Control, Communications, and Intelligence, Security & Information Operations
CERT	Computer Emergency response Team
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CMDS	Computer Misuse Detection System
CI	counterintelligence
CINC	Commander in Chief
COMSEC	Communications Security
COTS	Commercial Off The Shelf
DAA	Designated Approving Authority
DARPA	Defense Advanced Research Projects Agency
DASD(I)	Deputy Assistant Secretary of Defense (Intelligence)
DCI	Director of Central Intelligence
DCII	Defense Central and Investigations Index (DCII)
DDR&E	Director of Defense Research and Engineering
DIA	Defense Intelligence Agency
DIAC	Defense Intelligence Analysis Center
DIAP	Defense-Wide Infrastructure Assurance Program
DIRNSA	Director, National Security Agency
DISA	Defense Information Systems Agency DSS
DITSCAP	DoD Information Technology Security Certification & Accreditation Process
DoD	Department of Defense
DSS	Defense Security Service
EAP	Employee Assistance Program
EC	Electronic Commerce
EDI	Electronic Data Interchange
FFRDC	Federally Funded Research and Development Center
GOTS	Government Off The Shelf
GPRA	Government Performance and Results Act
I&W	indications and warning
IA	information assurance
IDS	Intrusion Detection System
INFOSEC	information security
IPT	Integrated Process Team
IS	Information System
ISP	Internet Service Provider
ISSO	Information System Security Officer
ISSM	Information System Security Manager

IT	Information Technology
LAC	Local Agency Check
NAC	National Agency Check
NACI	National Agency Check plus Written Inquiries
NACLC	National Agency Check with Local Agency Check
NSA	National Security Agency
NIAP	National Information Assurance Partnership (NIAP)
NSTISSC	National Security Telecommunications and Information Systems Security Committee
OGA	other government agencies
OGC	Office of General Counsel, OSD
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OSD	Office of the Secretary of Defense
OUSD	Office of the Undersecretary of Defense
PKI	Public Key Infrastructure
PR	Periodic Reinvestigation
R&D	research & development
SBU	Sensitive But Unclassified
SCO	Senior Civilian Official
SF-85PS	Standard Form - 85 Supplemental Questionnaire for Selected Positions
SSBI	Single Scope Background Investigation
SRC	Security Research Center, OSD / P&R

Endnotes

[1] OASD(C3I) memo, "Insider Threat Integrated Process Team (IPT)," Dec. 22, 1998.

[2] Automated Information Systems: Threats & Vulnerabilities, National Counterintelligence Center, Unclassified.

[3] Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, Unclassified.

[4] Technology Collection Trends in the US Defense Industry, Defense Security Service, 1999.

[5] DoD Office of the Inspector General, "DoD Management of Information Assurance Efforts to Protect Automated Information Systems," Report No. PO 97-049, September 25, 1997.

[6] "Insider Threats to Critical Information Systems" identifies eight types of perpetrators of malicious activity. Political Psychology Associates, Ltd., Contract #98-G-7900, August 31, 1999.

[7] No distinction is made here between the disgruntled employee and the agent provocateur.

[8] The Insider Threat IPT working groups and members submitted nearly one hundred twenty recommendations. By elimination or combination of similar recommendations, the current set contains sixty-five recommendations.

[9] Computer Science and Telecommunications Board, National Research Council

[10] NSTISSD #500, "Information Systems Security (INFOSEC) Education, Training and Awareness," February 23, 1993 and DoDD S-3600, "Information Operations," December 9, 1996.

[11] Recommendations are referenced to Appendix A.

[12] Information Assurance and Information Technology Human Resources IPT, "Information Assurance and Information Technology: Training, Certification, and Personnel Management in The Department of Defense," July 9, 1999.

[13] Intrusion Detection Systems (IDS) is a commonly used term within the discipline of Information Assurance. IDS is not entirely appropriate with regard to the insider issue in that insiders are not considered as intruding. The terms Anomaly and Misuse Detection Systems (see Glossary (Appendix C)), albeit more appropriate, are less commonly used and are usually categorized under IDS. IDS terminology will continue to be used in this report because of its widespread acceptance and usage.

[14] Richard Haver, Information Operations Symposium, San Diego, CA, Oct. 27,1999.

[15] Attorney General of the United States, Industry Advisory Council Conference, Richmond, VA, October 1998

[16] MG Raduege, Information Operations Symposium, San Diego, CA, Oct. 27, 1999

[17] Examples include DoDD 5200.28 and DoD 5200.1-R. Services, Combatant Commands and Agencies also have CJSCI 6510.1B.

[18] IA and IT Human Resources IPT, "Information Assurance and Information Technology: Training, Certification, and Personnel Management in the Department of Defense," July 9, 1999, and "The Department of Defense World Wide Web Security Training Guidance Requirements."