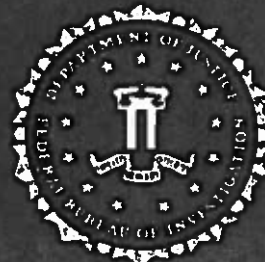


**(U) The United States
Government-Wide Cyber
Counterintelligence Plan**

2008



Foreword (U)

(U) The President's *Comprehensive National Cybersecurity Initiative* directs us to secure the cyber networks that make up our government's "central nervous system." This *Cyber Counterintelligence Plan* is part of that undertaking and fits seamlessly within the current *National Counterintelligence Strategy*.

(U) Protecting "cyberspace" requires that we reconsider the entire technical infrastructure involved in electronic communications. Protecting it will require a robust public-private effort because much of that infrastructure is privately owned. Moreover, the threats to our cyber operations may be enabled through remote electronic operations or by a human penetration or supply chain operation. This *Counterintelligence Cyber Plan* is therefore designed to address the full spectrum of threats.

(U) Much of what constitutes counterintelligence or "CI," and the many related activities that support counterintelligence, exist in organizations that are not designated as such. Counterintelligence is defined as "information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, foreign organizations or persons, or their agents, or international terrorist organizations or activities." While intelligence agencies all have a CI effort, the size of the human and financial resources focused on the CI business area is often small compared to other mission areas. As we embark on a Comprehensive National Cyber Security Initiative, we have been proactive and strategic in including CI in the formative stage. As the Initiative matures, we must remain committed to resourcing CI as a key aspect of our implementation, and we must align resources to each agency according to their responsibilities.

(U) We cannot sit back and monitor hostile cyber activities as they come. The volume, variety, and velocity of such activities are too great for such a passive strategy to work, and perimeters are electronically penetrable even by moderately sophisticated adversaries. Moreover, hostile cyber activities may be launched from inside network perimeters. This strategy therefore calls for a defense-in-depth. We will strengthen defenses at the edges of our networks and within our networks, building and strengthening electronic strong points where our most important information and system functionality resides. We will also gather intelligence on the source and nature of hostile cyber activities *before* they come. [REDACTED]

(b)(3)

(U) Foreign cyber penetrations that may receive the most public attention may not be the intrusions of the highest national security concern. The fact that we know about an intrusion suggests on its face that the intruder is not operating at the level of covert sophistication of which our most advanced adversaries are capable. Sophisticated, state-sponsored hostile cyber activities can appear to be invisible because they hide in the noise of continuous activities against U.S. systems. Cleaning the noise out of our systems is

important not only for its own sake, but also because doing so will make it easier to find the most insidious, currently invisible hostile cyber activities, which are far more dangerous.

(U) In the area of cyber counterintelligence, this *Plan* is the beginning of the extended effort that the President called for in his *Comprehensive National Cybersecurity Initiative*. In the national interest, it must be followed by concerted efforts that extend across the entire government and from one administration to the next.

Joel F. Brenner
National Counterintelligence Executive

John S. Pistole
Deputy Director
Federal Bureau of Investigation

Table of Contents

Table of Figures (U) v

Table of Tables (U) v

The Threat (U) 1

Background (U) 5

Outline of the Cyber CI Plan (U//FOUO) 8

Cyber Counterintelligence Objectives (U) 9

OBJECTIVE 1: Detect, deter, disrupt, and mitigate internal and external cyber threats through defensive counterintelligence measures. (U) 9

 Objective 1.1: *Detect, deter, disrupt, and mitigate internal threat. (U)* 10

 Objective 1.2: *Detect, deter, disrupt, and mitigate external threat. (U)* 12

OBJECTIVE 2: [REDACTED] (U) 12

 Objective 2.1: [REDACTED] (U) 13

 Objective 2.2: [REDACTED] (S//REL TO USA, FVEY) 14

 Objective 2.3: [REDACTED] (U) 15

OBJECTIVE 3: [REDACTED] (S) 16

 Objective 3.1: [REDACTED] (U//FOUO) 17

 Objective 3.2: [REDACTED] (TS//SI//NF) 18

OBJECTIVE 4: Strengthen collaboration among security, law enforcement, and counterintelligence elements. (U) 18

 Objective 4.1: *Infuse CI into existing security and law enforcement (LE) incident reporting. (U)* .. 19

 Objective 4.2: *Employ CI, LE, and cybersecurity methodologies to optimize responses. (U)* 19

 Objective 4.3: *Share CI information at the lowest classification possible. (U)* 20

 Objective 4.4: *Establish uniform incident reporting and forensic examination requirements. (U)*.. 20

OBJECTIVE 5: Conduct all-source counterintelligence analysis in support of the Cyber CI mission. (U) 21

 Objective 5.1: *Conduct Cyber CI analysis and provide actionable reporting. (U)* 22

 Objective 5.2: *Develop and coordinate cyber damage/loss assessments. (U)* 22

OBJECTIVE 6: Establish/expand Cyber CI education/awareness programs and workforce development to integrate counterintelligence into all aspects of cyber operations and analyses. (U) 23

 Objective 6.1: *Educate and train CI professionals about the full spectrum of cyber threats. (U)* 23

 Objective 6.2: *Expand national awareness on the threat posed by foreign adversaries. (U)* 24

Conclusion (U) 25

Appendix A: Resources (U) 26

Appendix B: Tools, Tradecraft, and Technology (U) 35

Appendix C: Assessment of Damage/Loss from Cyber Intrusions (U)... 42

Glossary (U) 46

(b)(3)

(b)(1)
(b)(3)

(b)(1)
(b)(3)

Table of Figures (U)

(b)(1)
(b)(3)

Figure 1: Threat Vectors (U)..... 1
Figure 2: [REDACTED] (S//REL TO USA FVEY)..... 6
Figure 3: [REDACTED] (S//REL TO USA FVEY)..... 6
Figure 4: [REDACTED] (S//REL TO USA FVEY)..... 8
Figure 5: [REDACTED] (U//FOUO)..... 45

Table of Tables (U)

(b)(1)
(b)(3)

Table 1: Observations and Recommendations (U)..... 4
Table 2: [REDACTED] (S//NF)..... 26
Table 3: [REDACTED] (S//NF)..... 27
Table 4: [REDACTED] (S//NF)..... 31
Table 5: [REDACTED] (S//NF)..... 31
Table 6: [REDACTED] (S//NF)..... 33
Table 7: [REDACTED] (S//NF)..... 34
Table 8: [REDACTED] (S//NF)..... 34

The Threat (U)

(b)(1)
(b)(3)

~~(TS//SI//NF)~~

(U//FOUO) Trusted insiders as well as external adversaries are targeting all aspects of cyberspace – a global domain within the information environment consisting of interdependent networks of information technology infrastructures, which include the Internet, telecommunications networks, computer systems, and embedded processors and controllers – for exploitation, disruption, and potential destruction. Threats include vendor and supply chain exploitation, remote access operations, close access technical operations, and insider exploitation. Potential damage ranges from theft or alteration of data to denial of service or the destruction of cyber assets.

(U//FOUO) Figure 1: *Threat Vectors* (U) describes access methods that are used to exploit U.S. Government networks. The vendor/supply chain threat represents one end of the spectrum where adversarial access can occur anywhere within a broad continuum. The other end of the threat spectrum is represented by insider access, which typically points to one individual. Regardless of where the threat originates, the consequence is the same: a serious disruption to U.S. national security and economic stability. These threats are explained more fully below.

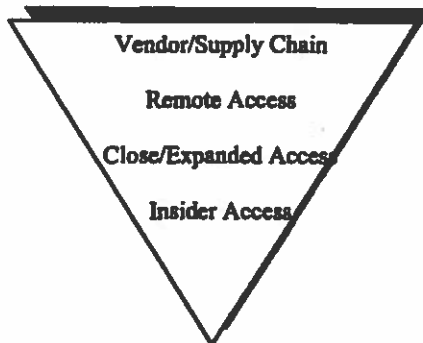


Figure 1: Threat Vectors (U)

¹ (U) Source: 2004-01 National Intelligence Estimate, "Cyber Threats to the U.S. Information Infrastructure."

Exploitation of the vendor/supply chain: (U) Operations to gain advantage, control, and/or access to intelligence information and/or information systems through manipulation of hardware and/or software by cooperative vendors, or unilaterally during any point in the supply chain from system design through installation at the end user site to include servicing and retirement.

~~(S//REL TO USA FVEY)~~

(b)(1)
(b)(3)

[REDACTED]

Remote (network) access: (U) Operations to access target information and/or information systems through network-based technical means.

~~(TS//SI//NF)~~

(b)(1)
(b)(3)

[REDACTED]

Close/expanded access: (U//FOUO)

(b)(7)(E)

[REDACTED]

~~(S)~~

(b)(1)
(b)(3)

[REDACTED]

(b)(3)

[REDACTED]

(b)(1)
(b)(3)

[REDACTED]

Insider threat: (U//FOUO) Operations involving the witting or unwitting unauthorized use or access to information, systems, and networks by otherwise trusted agents (employees), for the purposes of either collection or manipulation.

(U//FOUO) Trusted insiders can steal information electronically or facilitate remote access to unprecedented amounts of data and they may be ideally positioned to inflict devastating damage to U.S. Government networks through espionage and/or sabotage. According to the 2004 e-Crime Watch Survey, in cases where the perpetrator of an electronic crime or intrusion could be identified, a considerable number were committed by insiders.⁴

(U//FOUO) [REDACTED]

(b)(3)

What the U.S. should do: (U)

(U//FOUO) Although the U.S. Government is making strides in securing government networks and protecting the supply chain, determined adversaries will increasingly adapt their methods to overcome security constraints - [REDACTED]

(b)(3)

[REDACTED]

(b)(1)
(b)(3)

³ (S) [REDACTED]

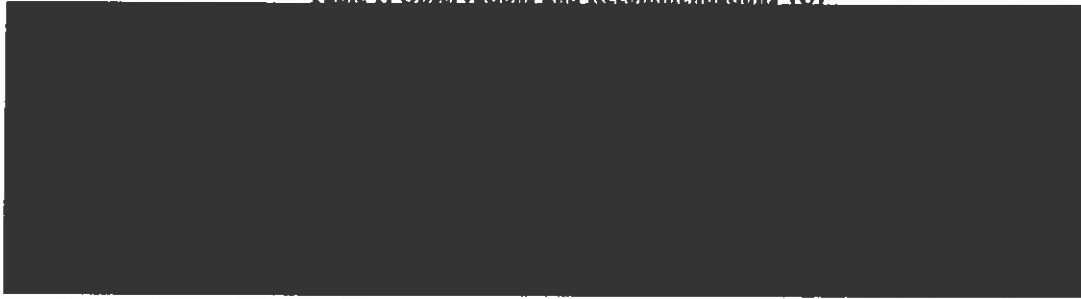
⁴ (U) 2004 eCrime Watch Survey, conducted by CSO magazine in cooperation with the U.S. Secret Service and CERT Coordination Center.

(b)(3)

[REDACTED]

(b)(3)

Table 1: Observations and Recommendations (U)



Background (U)

(U) The National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23)⁶ directed the Attorney General (AG) and the Director of National Intelligence (DNI) to develop a comprehensive Cyber Counterintelligence (Cyber CI) plan, including required resources. The AG and DNI delegated this responsibility to the Federal Bureau of Investigation (FBI) and the Office of the National Counterintelligence Executive (ONCIX).

(U) For the purposes of this plan, cyber counterintelligence is defined as counterintelligence, by any means, where a significant target or tool of the adversarial activity is a computer, computer network, embedded processor or controller, or the information thereon.

(U) The Cyber CI plan builds on the Presidentially approved *National Counterintelligence Strategy of the United States of America (2007)* and supports the following National Counterintelligence Mission and Enterprise Objectives:

- (U) Exploit and defeat adversarial intelligence activities directed against U.S. interests.
- (U) Protect the integrity of the U.S. Intelligence System.
- (U) Provide incisive, actionable intelligence to decision makers at all levels.
- (U) Protect vital national assets from adversarial intelligence activities.
- (U) Neutralize and exploit adversarial intelligence activities targeting the Armed Forces.⁷
- (U) Strengthen the counterintelligence cadre.
- (U) Expand national awareness of adversarial intelligence threats.

(S//REL TO USA, FVEY) The Cyber CI plan is an integral component of the *Comprehensive National Cybersecurity Initiative (CNCI)*, which establishes U.S. policy, strategy, guidelines, and implementation actions to secure cyberspace.

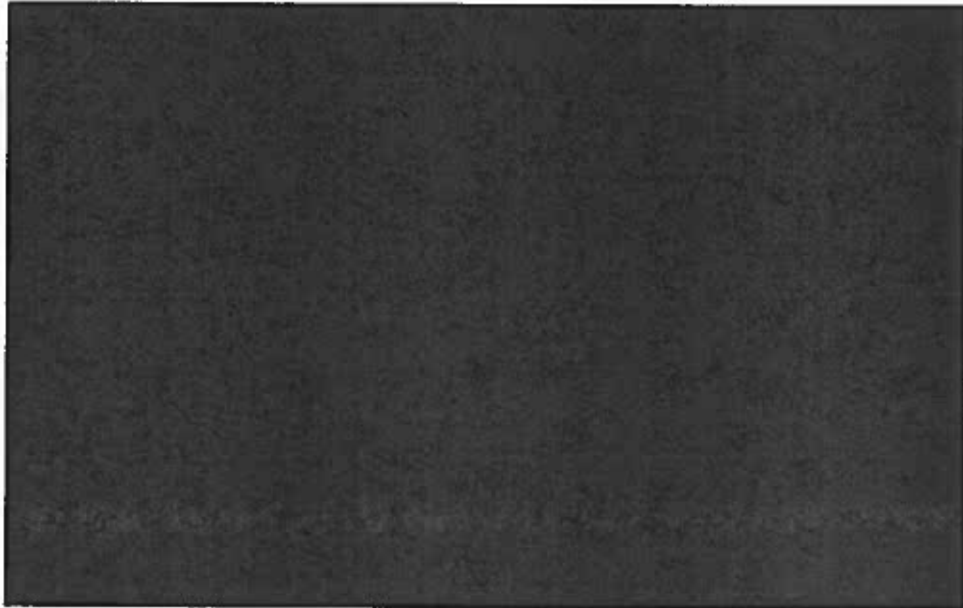
(b)(1)
(b)(3)

(S//REL TO USA, FVEY)
(S//REL TO USA, FVEY)

⁶ (U) *Cybersecurity Policy*, 8 January 2008

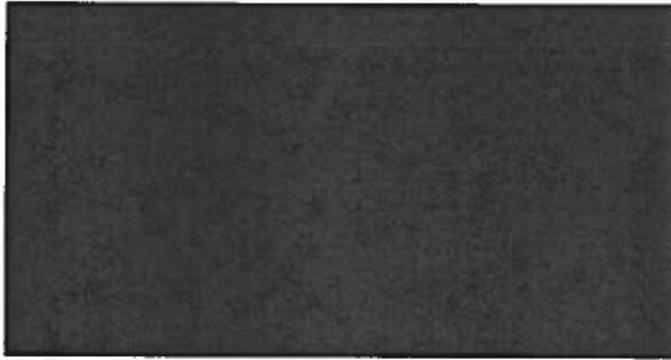
⁷ (U) The DoD Cyber Counterintelligence Strategy of 2008 is a critical enabling element of this plan.

(b)(1)
(b)(3)



~~SECRET//REL TO USA, FVEY~~

Figure 2: The 12 Interdependent Cybersecurity Initiatives (~~SI//REL TO USA FVEY~~)



~~SECRET//REL TO USA, FVEY~~

Figure 3: The 7 Interdependent Strategic Enablers (~~SI//REL TO USA FVEY~~)

(b)(7)(E)

(U) The Cyber CI plan calls for unity of effort across the U.S. Government.

(U) To safeguard the privacy and civil liberties of U.S. citizens, residents, and organizations, each participating organization will operate under its existing authorities and policy/security frameworks, and will consult with offices of general counsel and privacy and civil liberties officers, as appropriate, to ensure compliance with law and with Attorney General approved guidelines safeguarding U.S. persons. Further, all activities contemplated by the Cyber CI Plan will be conducted in accordance with relevant statutes, Executive Orders, and U.S. Government regulations governing the

dissemination of intelligence-related information. This will allow the greatest flexibility while maintaining a high level of public trust.

(U) Proposed FY09-FY13 resources for implementation of the Cyber CI Plan are allocated to ONCIX, the Central Intelligence Agency, and the Department of Defense. See Appendix A for a detailed discussion of the proposed resources and deliverables.

Outline of the Cyber CI Plan (U//FOUO)

The Cyber CI Objectives are shown in Figure 4:

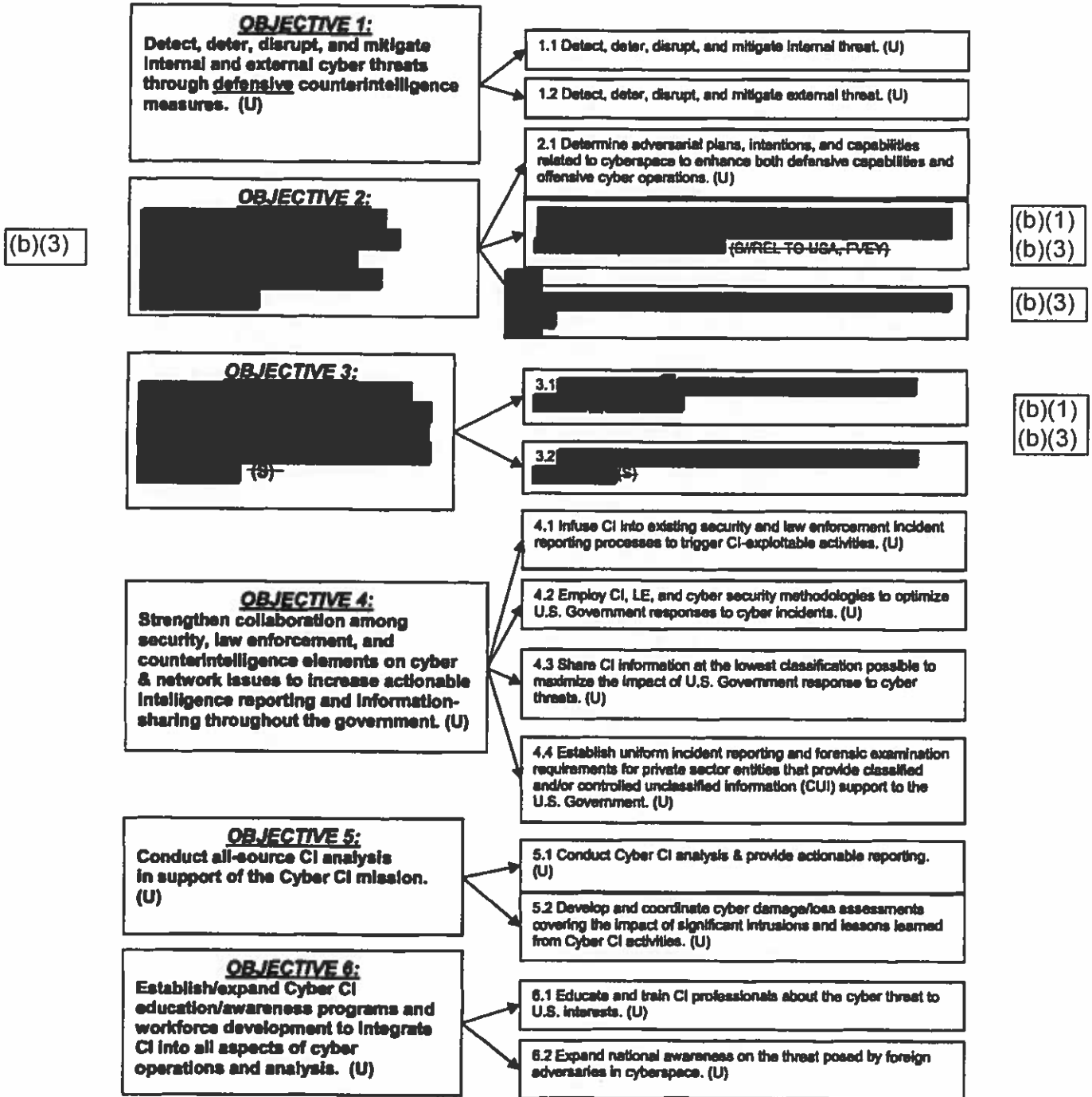


Figure 4: Cyber CI Plan Objectives (S//REL TO USA FVEY)

Cyber Counterintelligence Objectives (U)

OBJECTIVE 1: Detect, deter, disrupt, and mitigate internal and external cyber threats through defensive counterintelligence measures. (U)

(b)(3)

(U//FOUO) [REDACTED]

(U//FOUO) [REDACTED]

(b)(3)

(U//FOUO) U.S. Government networks (both unclassified and classified) are constantly targeted by cyber intruders. Efforts by foreign intelligence and security services (FISS) to infiltrate these networks and exfiltrate sensitive data on a massive scale, or to spot, assess, and recruit U.S. citizens ("insiders") in carrying out their intelligence missions is well documented. Adversaries look to exploit any weakness. The U.S. must strengthen its defense-in-depth strategy by enhancing perimeter and internal core defenses; [REDACTED]

(b)(3)

(U//FOUO) Network defense assets exist throughout the U.S. Government as a basic component of network administration. [REDACTED]

(b)(3)

[REDACTED] While the Cyber CI community does not develop or implement policies, procedures, or tools related to network defense and information assurance – that is beyond its scope – it does investigate cyber incidents, support operations against hostile cyber activities, produce damage assessments, and prepare threat assessments or reports. To better support defensive measures, the Cyber CI community must expand on those traditional mission sets and add others, [REDACTED]

(b)(3)

(e) [REDACTED]

(b)(1)

(b)(3)

(b)(1)
(b)(3)

[REDACTED]

(U//FOUO) The following sub-objectives will contribute to the success of Objective 1:

Objective 1.1: *Detect, deter, disrupt, and mitigate internal threat.* (U)

(S//REL TO USA, FVEY)

[REDACTED]

(b)(1)
(b)(3)

(S//REL TO USA, FVEY)

[REDACTED]

(b)(1)
(b)(3)

(S//NF)

[REDACTED]

(b)(1)
(b)(3)

(b)(3)

[REDACTED]

¹⁰ (U) Per Appendix B, these tools will be catalogued and shared as appropriate.

¹¹ (U) See Appendix B.

(b)(1)
(b)(3)

[REDACTED]

(b)(1)
(b)(3)

(S//NF)
[REDACTED]

(b)(1)
(b)(3)

(S//REL TO USA, FVEY)
[REDACTED]

(b)(7)(E)

(U//FOUO) The insider threat is not limited to U.S. Government agencies and organizations; private industry is also at risk. To gain access to classified or sensitive U.S. Government information (including information in the critical development stages of technology lifecycles), [REDACTED]
[REDACTED] Compounding the problem, private industry has less stringent incident reporting and network-monitoring requirements than U.S. Government

(b)(3)

[REDACTED]

agencies, and may be disinclined to share this type of information for financial and legal liability reasons. The Cyber CI community, in coordination with the Department of Homeland Security (DHS), will engage its industry partners to improve the understanding of the insider threat and will share knowledge of current best practices and emerging technologies to audit and monitor systems and networks. Outreach personnel will ensure their corporate partners are aware that an unclassified version of the current economic espionage report is available for download at <http://www.ncix.gov/publications/reports/index.html>.

Objective 1.2: *Detect, deter, disrupt, and mitigate external threat.* (U)

(S//NF) [REDACTED]

(b)(1)
(b)(3)

(S//REL TO USA, FVEY) [REDACTED]

(b)(1)
(b)(3)

(b)(3)

OBJECTIVE 2: [REDACTED] (U)

(b)(7)(E)

(U//FOUO) This objective responds to the tasking outlined in the [REDACTED] and aligns with the *National Counterintelligence Strategy's Mission*

¹³ (U) This plan is called for in paragraph 49 of NSPD-54/HSPD-23.

(b)(3) Objective 1: [REDACTED]

(U//FOUO) [REDACTED]
(b)(3) [REDACTED]

(E) [REDACTED]
(b)(1) [REDACTED]
(b)(3) [REDACTED]

(E) [REDACTED]
(b)(1) [REDACTED]
(b)(3) [REDACTED]

(U//FOUO) [REDACTED]
(b)(3) [REDACTED]

(U//FOUO) The following sub-objectives will contribute to the success of Objective 2:

(b)(3) Objective 2.1: [REDACTED]
[REDACTED] (U)

(b)(1) (TS//NF) [REDACTED]
(b)(3) [REDACTED]

(b)(1)
(b)(3)

[REDACTED]

~~(S//REL TO USA, FVEY)~~

(b)(1)
(b)(3)

[REDACTED]

(b)(1)
(b)(3)

Objective 2.2:

[REDACTED]
(S//REL TO USA, FVEY)

~~(S//NF)~~

(b)(1)
(b)(3)

[REDACTED]

(b)(1)
(b)(3)

~~(TS//NF)~~

[REDACTED]

(b)(3)

[REDACTED]

(b)(1)
(b)(3)

[REDACTED]

(S//REL TO USA, FVEY)

(b)(1)
(b)(3)

[REDACTED]

(b)(3)

Objective 2.3: [REDACTED]
[REDACTED] (U)

(TS//NF)

(b)(1)
(b)(3)

[REDACTED]

(b)(1)
(b)(3)

(S)

[REDACTED]

(S//NF)

(b)(1)
(b)(3)

[REDACTED]

(b)(3)

¹⁶ (S)
¹⁷ (S)

[REDACTED]

(S) [Redacted]

(b)(1)
(b)(3)

OBJECTIVE 3: [Redacted]
[Redacted] (S)

(b)(1)
(b)(3)

(U//FOUO) This Objective aligns with the *National Counterintelligence Strategy's* Mission Objective 4: [Redacted]

(b)(3)

(U//FOUO) This Objective also links to CNCI Initiative 11 [Redacted]
[Redacted]

(b)(3)

(U) The globalization of business has increased the role of international companies and foreign vendors in the U.S. IT supply chain. Fiscal savings derived from outsourcing services such as life cycle maintenance have driven many U.S. firms to outsource activities to foreign companies.

(b)(1)
(b)(3)

~~(S//REL TO USA, FVEY)~~ [Redacted]

(b)(1)
(b)(3)

¹⁹ (S) [Redacted]

(U//FOUO) The CI threat to the supply chain can occur at any stage of a product's lifecycle – from design to manufacture, from distribution to maintenance or retirement.

(b)(3)

(U) The following sub-objectives will contribute to the success of Objective 3:

Objective 3.1:

(b)(3)

~~(U//FOUO)~~

~~(S//REL TO USA, FVEY)~~

(b)(1)
(b)(3)

(E)

(b)(1)
(b)(3)

~~(S//REL TO USA, FVEY)~~

(b)(1)
(b)(3)

(U//FOUO) [REDACTED]

(b)(3)

(S) [REDACTED]

(b)(1)
(b)(3)

Objective 3.2: [REDACTED]
[REDACTED] (TS//SI//NF)

(b)(1)
(b)(3)

(TS//SI//NF) [REDACTED]

(b)(1)
(b)(3)

OBJECTIVE 4: Strengthen collaboration among security, law enforcement, and counterintelligence elements on cyber and network issues to increase actionable intelligence reporting and information-sharing throughout the government. (U)

(U//FOUO) This Objective aligns with the *National Counterintelligence Strategy's* Mission Objective 2: [REDACTED]

(b)(3)

²⁰ (U) The CNSS provides a forum for the discussion of policy issues, sets national policy, and promulgates direction, operational procedures, and guidance for the security of national security systems.
²¹ (U) *Framework for Lifecycle Risk Mitigation For National Security Systems in the Era of Globalization*, 10 July 2006.

(S) [REDACTED]

(b)(1)
(b)(3)

(U//FOUO) The movement of sensitive information onto U.S. networks will continue to increase at an exponential rate. The security risk continuum is exceptionally broad and the risk posed by a [REDACTED]

(b)(3)

[REDACTED]. Network and computer security alone are not enough to keep U.S. interests secure. To enhance the integrity of U.S. networks and the information that resides on them, the U.S. Government needs to strengthen collaboration among security, law enforcement, and counterintelligence elements on cyber and network issues. This will require actionable intelligence reporting and information-sharing. [REDACTED]

(b)(3)

(U) The following sub-objectives will contribute to the success of Objective 4:

Objective 4.1: *Infuse CI into existing security and law enforcement (LE) incident reporting processes to trigger CI-exploitable activities. (U)*

(E) [REDACTED]

(b)(1)
(b)(3)

Objective 4.2: *Employ CI, LE, and cybersecurity methodologies to optimize U.S. Government responses to cyber incidents. (U)*

(E) [REDACTED]

(b)(1)
(b)(3)

(b)(3)

[REDACTED]

(b)(1)
(b)(3)

[REDACTED]

(S) [REDACTED]

(b)(1)
(b)(3)

Objective 4.3: Share CI information at the lowest classification possible to maximize the breadth of the U.S. Government's response to cyber threats.²³ (U)

(U//FOUO) To produce useful information for our cybersecurity and CI customers, it is critical to maintain the lowest possible classification level suitable to the subject while protecting sources and methods. Whenever practical, the Cyber CI community will institutionalize the use of tear lines to separate CI collection methods and analysis from public domain material [REDACTED]

(b)(7)(E)

[REDACTED] It is critical that vital information be disseminated as broadly and rapidly as possible, even at the expense of greater detail. The Cyber CI community will develop requirements for Initiative 8 (*Improve National Cyber Education and Expertise*) to ensure that analytical training modules include a segment on how to balance classification requirements and the "responsibility to provide" requirement when sharing CI information pertinent to cybersecurity. Classification does not always imply criticality. Unclassified intelligence can be extremely valuable when shared with LE and other partners so that it may have a greater impact on cybersecurity throughout the U.S. Government.

(b)(1)
(b)(3)

(S) [REDACTED]

Objective 4.4: Establish uniform incident reporting and forensic examination requirements for private sector entities (contractors, think tanks, academic

(b)(3)

²³ (U) See U.S. Intelligence Community Information Sharing Strategy, 22 February 2008.

institutions) that provide classified and/or Controlled Unclassified Information (CUI)²⁵ support to the U.S. Government. (U)

(S//NF) [REDACTED]

(b)(1)
(b)(3)

(C) [REDACTED]

(b)(1)
(b)(3)

OBJECTIVE 5: Conduct all-source counterintelligence analysis in support of the Cyber CI mission. (U)

(U//FOUO) This Objective aligns with the *National Counterintelligence Strategy's* Objective 3: [REDACTED]

(b)(3)

(U//FOUO) This Objective also links to CNCI Initiative 5 ([REDACTED]) and the *National Cyber Security Center*.

(b)(3)

(U//FOUO) The difficulty of being able to rapidly and reliably attribute [REDACTED]. The Cyber CI mission requires data fusion and analysis from multiple sources, including LE, cybersecurity, and CI community information in order to [REDACTED]. All-source CI analysis and cyber damage assessments are essential to determine [REDACTED] and contribute to the success of the Cyber CI mission. [REDACTED], even if

(b)(3)

²⁵ (U) "Controlled unclassified information" term replaced "sensitive but unclassified" term per White House *Designation and Sharing of Controlled Unclassified Information* memo, 7 May 2008.

(b)(3)

assessments are tentative. Policy makers will need to make decisions quickly, despite not having a "perfect" answer. [REDACTED]

(U) The following sub-objectives will contribute to the success of meeting Objective 5:

Objective 5.1: Conduct Cyber CI analysis and provide actionable reporting.
(U)

(b)(3)

(U//FOUO) [REDACTED]

Objective 5.2: Develop and coordinate cyber damage/loss assessments covering the impact of significant intrusions and lessons learned from Cyber CI activities. (U)

(U//FOUO) [REDACTED]

(b)(3)

- (U) [REDACTED]
- (U) [REDACTED]

(b)(3)

(b)(3)

²⁶ (U//FOUO) See Appendix C, [REDACTED] January 31, 2008.

(b)(3)

- (U) [REDACTED]
- (U) [REDACTED]

OBJECTIVE 6: Establish/expand Cyber CI education/awareness programs and workforce development to integrate counterintelligence into all aspects of cyber operations and analyses. (U)

(b)(3)

(U//FOUO) This Objective aligns with the *National Counterintelligence Strategy's* Enterprise Objectives 2 and 3: [REDACTED]

(b)(3)

(U//FOUO) This Objective also links to CNCI Initiative 8 [REDACTED]

(b)(3)

(U//FOUO) The United States must improve its technical cyber skills to prevail in cyberspace. [REDACTED] Cybersecurity training and education will cover the spectrum from the need for general awareness on the part of each government employee to the unique needs of law enforcement, intelligence, the military, homeland security, and other mission managers. The Cyber CI community will develop requirements for CNCI Initiative 8 [REDACTED] for development of education and awareness programs to enable the cyber workforce to understand and more effectively integrate the Cyber CI mission throughout government cyber and CI programs.

(b)(3)

(U//FOUO) The creation of a government training and education program that integrates counterintelligence in all aspects of computer network and cybersecurity operations should result in more effective and agile Cyber CI activities. Increasing awareness of the cyber threat and mitigation mechanisms to protect against those threats [REDACTED]

(U) The following sub-objectives will contribute to the success of Objective 6:

Objective 6.1: Educate and train CI professionals about the full spectrum of cyber threats to U.S. interests. (U)

(b)(3)

(U//FOUO) The ONCIX-published documents [REDACTED] These community-coordinated documents will be used when integrating cyber-

specific training into existing counterintelligence training programs. As universal cyber competencies are validated, they will be reflected in updated editions of the above documents. To ensure long-term success, the CI workforce must enhance and continually refresh its cyber expertise and impart this knowledge throughout CI analytic, operational, and investigative agencies and departments.

~~(S//NF)~~ [REDACTED]

(b)(1)
(b)(3)

~~(S//NF)~~ [REDACTED]

(b)(1)
(b)(3)

Objective 6.2: Expand national awareness on the threat posed by foreign adversaries in cyberspace. (U)

(U//FOUO) Guided by existing U.S. cyber-related training and education programs, the Cyber CI community will develop Cyber CI modules for integration into national cyber curriculums. These modules will expose government cyber professionals to the broad range of CI threats that exist in cyberspace and help them mitigate those risks in their day-to-day operations. Outreach and awareness efforts to non-IC agencies, the private sector, and academia will complement Cyber CI training efforts and will contribute to a more informed understanding of the cyber threat in the government acquisition community. Outreach to the private sector will be conducted by the Sector Specific Agencies as established by the NIPP.

(U//FOUO) Given the wide range of Cyber CI customers (e.g. system administrators, users, owners, hardware and software developers, lawyers, procurement officers, and intelligence collectors), the Cyber CI community will develop training appropriate to user type and identify reference materials to be used for each user class. [REDACTED]

(b)(3)

(b)(3)

Conclusion (U)

(U) These objectives chart the Cyber CI community's planning and operations activities and will provide the requirements for task prioritization and programmatic planning. The ONCIX, in consultation with the National Counterintelligence Policy Board and the Office of the Director of National Intelligence, will oversee implementation of the objectives through an integrated counterintelligence community effort using resources identified in Appendix A.

(U) The Cyber CI community acknowledges that each U.S. department or agency with cybersecurity and/or cyber CI responsibilities operates under legal authorities and policy guidelines relevant to its specific mission. This plan is not intended to intrude on those responsibilities or to redirect an organization's cyber CI operations. Mindful that no single entity can adequately address this threat in its entirety, the intent is rather to capitalize on each organization's unique capabilities so that the U.S. can respond to cyber CI threats with a coordinated approach.

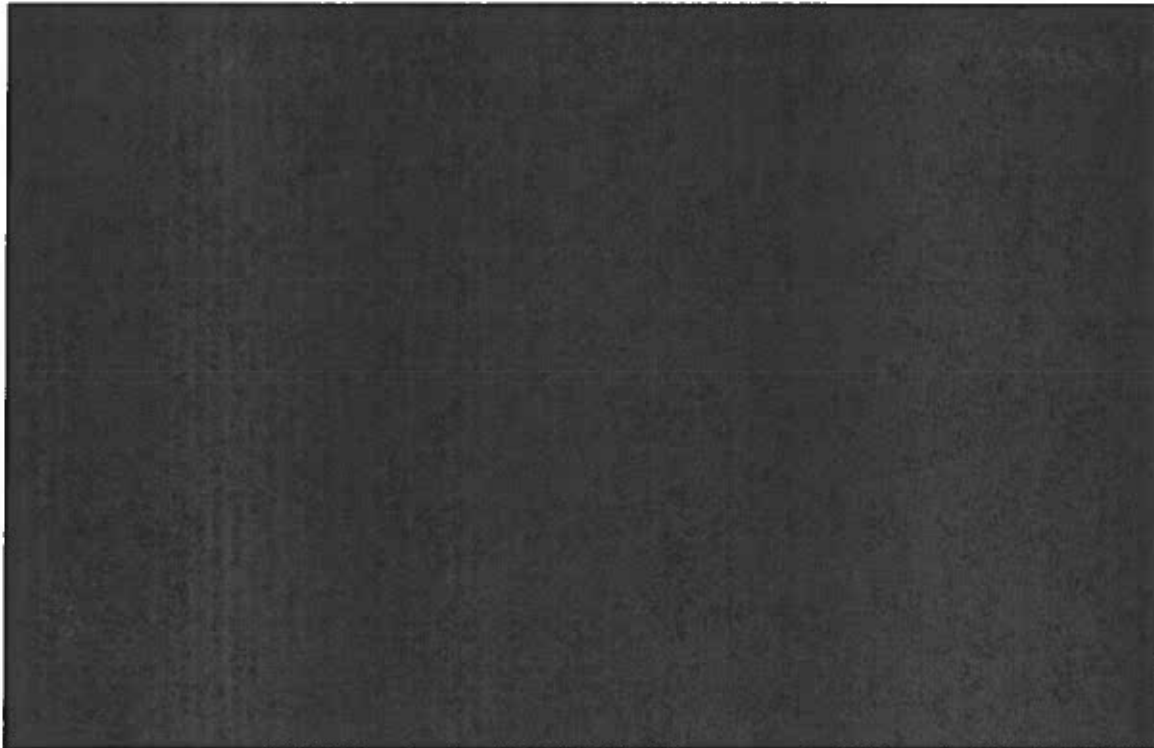
(U) The CI tools and techniques that will be developed as a result of this plan will be inherently sensitive, and any compromise will negate their effect. Accordingly, this plan acknowledges the need to properly protect these tools and techniques using established Intelligence Community security procedures and protocols.

Appendix A: Resources (U)

(U) The table below is a summary of FY09-13 resources needed, by Agency, to implement and oversee the deliverables outlined in *The United States Government-Wide Cyber Counterintelligence Plan*.

(b)(1)
(b)(3)


Table 2: Summary of Resources ~~(S//NF)~~



(U) **FY08 Funds:** There are no CNCI funds available for FY08. Current activities are being conducted with base funding.

(U) Spending Plan Breakdown by Organization

(U) ONCIX

(U) ONCIX will provide a detailed spend plan once the Cyber CI Plan is approved. In the interim, the summary below (by function) is how ONCIX will utilize its proposed FY09 and FY10 funds. The activities are linked to the proposed deliverables identified in Table 3:  ~~(S//NF)~~



(b)(1)
(b)(3)

~~(S//NF)~~ [Redacted]

(b)(1)
(b)(3)

~~(S//NF)~~ [Redacted]

(U) **Policy:** Maintain existing policies and update Cyber CI policies, procedures, standards and guidance, to address requirements for the USG Cyber CI community. Ensure the Cyber CI Plan is consistent with other USG cyber policies, strategies and implementation plans.

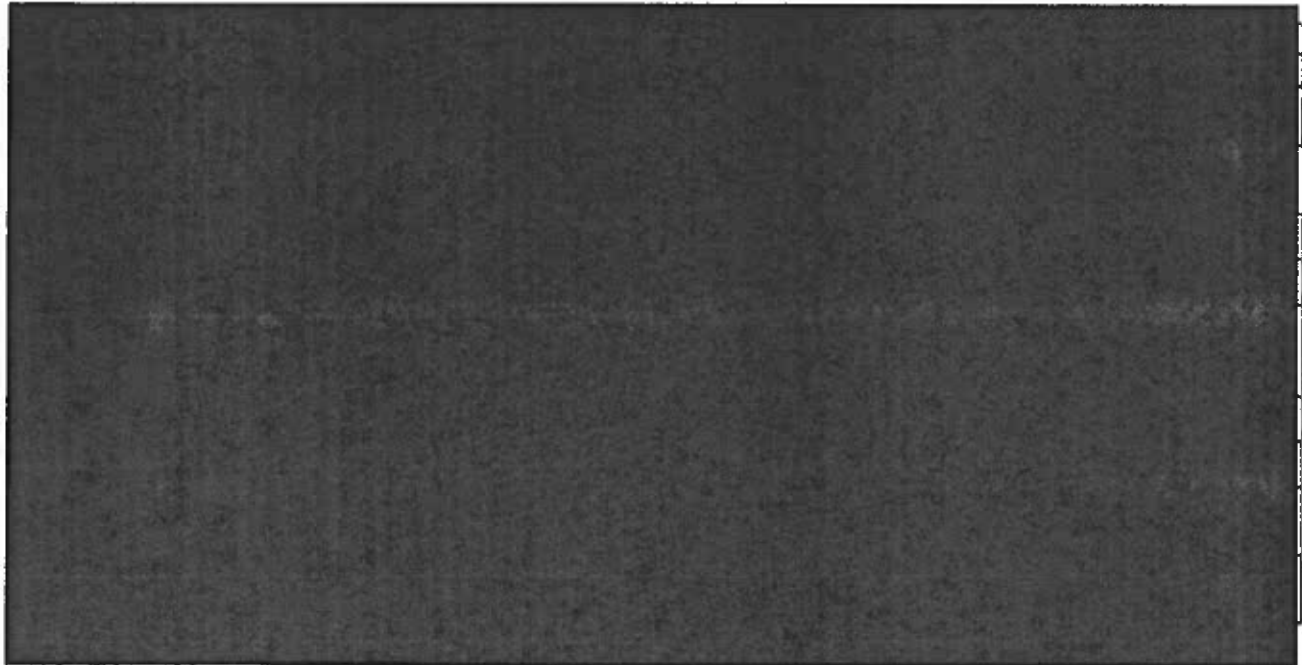
(U) **Training & Outreach:** Develop requirements for Cyber CI training. Identify appropriate cyber competencies for counterintelligence professionals. Formulate a Communication Strategy focusing on Cyber CI outreach efforts and marketing, to ensure stakeholder engagement and communication is consistent with the *National Counterintelligence Strategy of the United States of America*, and all pertinent USG working groups.

(b)(1)
(b)(3)

~~(S)~~ [Redacted]

(b)(1)
(b)(3)

Table 3: [Redacted] ~~(S//NF)~~

A large rectangular area of the page is completely redacted with a solid black fill, obscuring the content of Table 3.

(b)(1)
(b)(3)

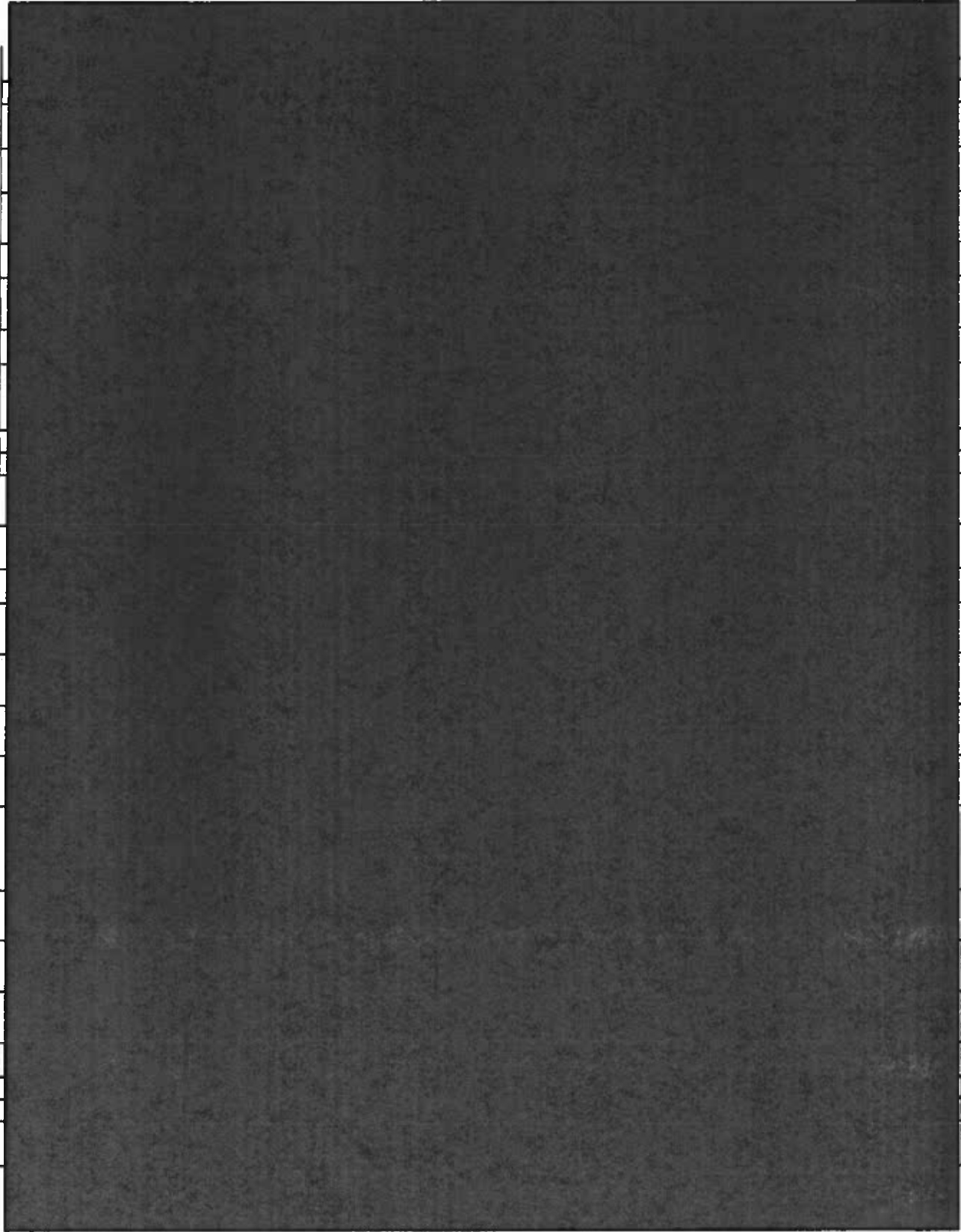
~~TOP SECRET//SI//NOFORN~~



~~TOP SECRET//SI//NOFORN~~

(b)(1)
(b)(3)

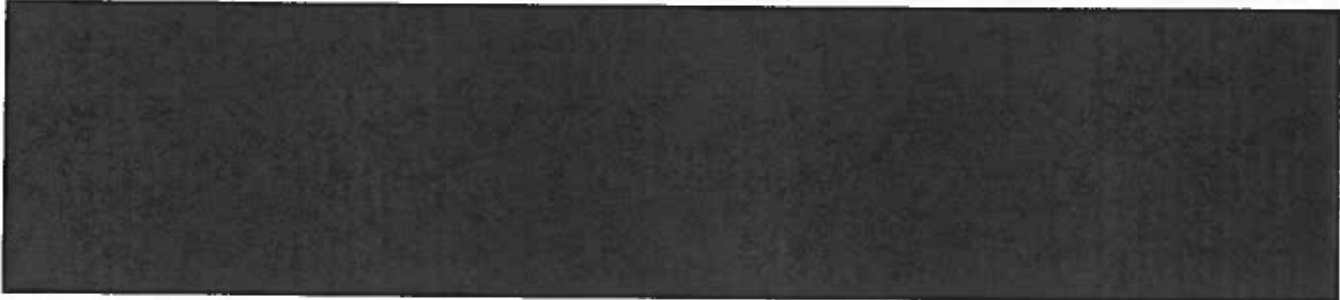
~~TOP SECRET//SI//NOFORN~~



~~TOP SECRET//SI//NOFORN~~

(b)(1)
(b)(3)

~~TOP SECRET//SI//NOFORN~~



~~TOP SECRET//SI//NOFORN~~

(b)(1)
(b)(3)

(U) CIA:

Table 4: [REDACTED] (S//NF)

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Table 5: [REDACTED] (S//NF)

(b)(1)
(b)(3)

~~TOP SECRET//SI//NOFORN~~

[REDACTED]

(S//NF) [REDACTED]

[REDACTED]

(S//NF) [REDACTED]

Cyber Tradecraft Program:

(S//NF) [REDACTED]

(S//NF) [REDACTED]

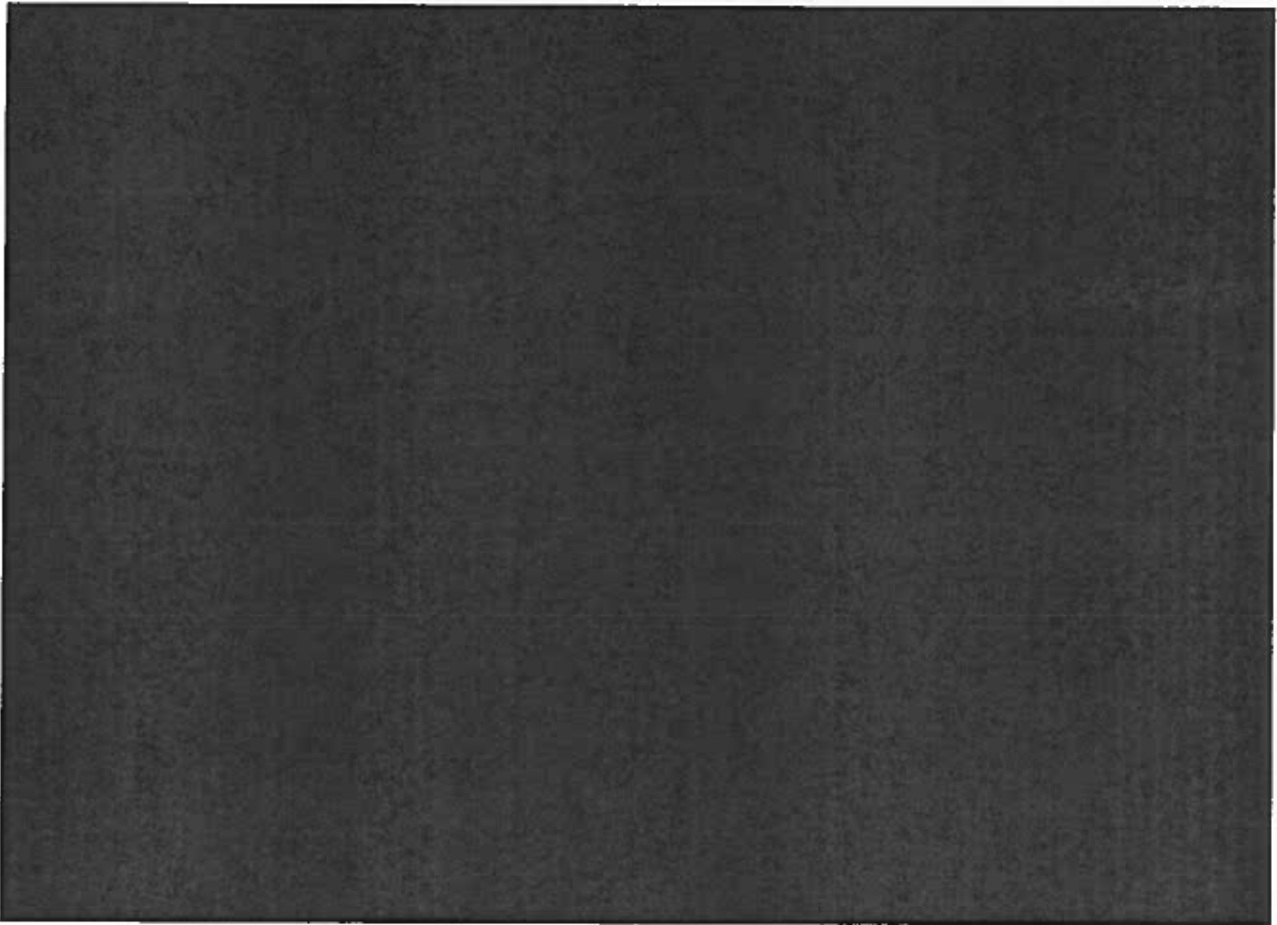
(S//NF) [REDACTED]

~~TOP SECRET//SI//NOFORN~~

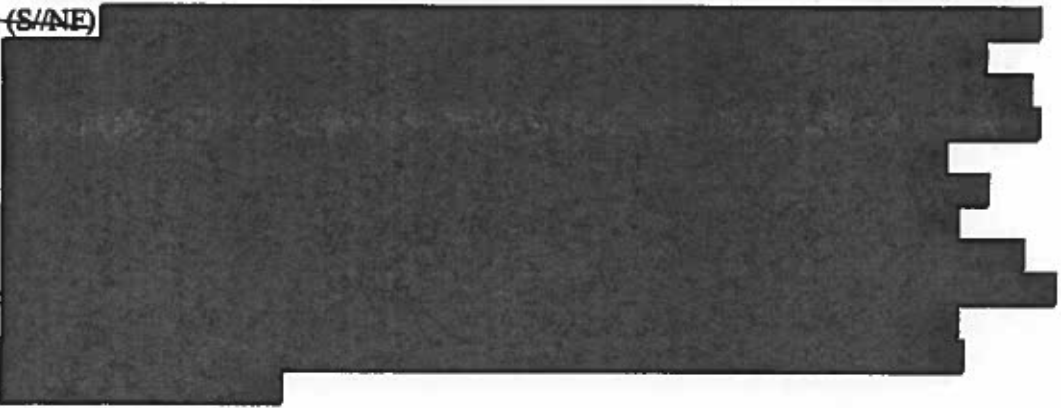
(b)(1)
(b)(3)

(U) DoD

Table 6:  ~~(S//NF)~~



~~(S//NF)~~ 

~~(S//NF)~~ 

(b)(1)
(b)(3)

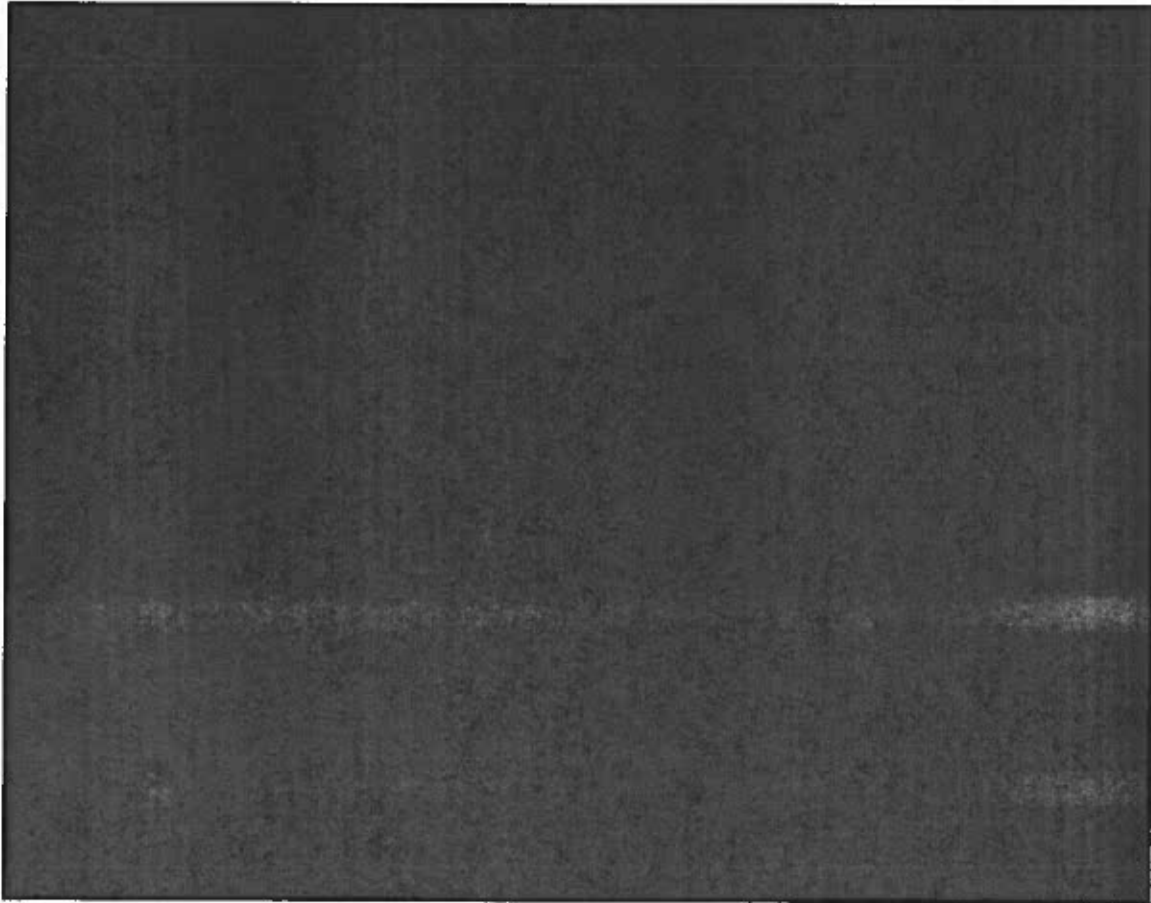
Personnel Staff

Table 7: [REDACTED]

~~(S//NF)~~



Table 8: [REDACTED] ~~(S//NF)~~



(b)(1)
(b)(3)

Appendix B: Tools, Tradecraft, and Technology (U)

(C) [REDACTED]

B1. [REDACTED]
(C)

(C) [REDACTED]

[REDACTED]

- (U) The [REDACTED] working group will accomplish the following:

(TS//SI//NF) [REDACTED]

(TS//SI//NF) [REDACTED]

(b)(1)
(b)(3)

[REDACTED]

(TS//NF)
[REDACTED]

(TS//SI//NF)
[REDACTED]

(b)(1)
(b)(3)

Technology Requirements:

B.2 Technical Requirements for Document Tagging, Tracking and Locating (TTL) Tools and Technology (Initiative 7, Initiative 9) (U)

(TS//NF) [Redacted]

(TS//NF) [Redacted]

- (TS//NF) [Redacted]

- (TS//NF) [Redacted]

- (TS//NF) [Redacted]

- (TS//NF) [Redacted]

- (TS//NF) [Redacted]

(b)(1)
(b)(3)

[REDACTED]

- ~~(TS//SI//NF)~~ [REDACTED]

- ~~(S//NF)~~ [REDACTED]

B.3 [REDACTED] ~~(C)~~

~~(S//NF)~~ [REDACTED]

- ~~(TS//SI//NF)~~ [REDACTED]

(b)(1)
(b)(3)

- ~~(TS//SI//NF)~~ [REDACTED]

- ~~(TS//SI//NF)~~ [REDACTED]

B.4 Technical Requirements for IC Department or Agency-specific and IC TS//SCI Fabric Enterprise-wide Audit Sharing Programs (U)

~~(TS//NF)~~ [REDACTED]

- ~~(TS//SI//NF)~~ [REDACTED]

³⁰ Intelligence Authorization Act for Fiscal Year 2009 Classified Annex

(b)(1)
(b)(3)

[REDACTED]

- (TS//SI//NF) [REDACTED]

B.5 Technical Requirements for Supply Chain Tools and Technology (U)

(TS//SI//NF) [REDACTED]

- (TS//SI//NF) [REDACTED]

- (TS//SI//NF) [REDACTED]

B.6 (U) Cyber Identification Friend or Foe

(TS//NF) [REDACTED]

(b)(1)
(b)(3)

- (TS//NF) [REDACTED]
- (TS//NF) [REDACTED]

Appendix C: Assessment of Damage and Loss from Cyber Intrusions (U)

What is a damage or loss assessment? (U)

(U) Cyber damage or loss assessments are systematic, comprehensive reviews of intentional and/or inadvertent compromises of sensitive or classified information. Such assessments build on incident reporting and can cover single incidents or the combined effects, loss, or lessons learned from a combination or series of incidents. To be effective, loss assessments must be timely and should produce outputs in phases. Outputs should include mitigation recommendations both for short term response actions as well as long term options and implications. The customers of a cyber loss assessment are the owners, custodians, and users of the data, as well as network operators and defenders and those building knowledge bases on adversarial capabilities and tactics. Since the length of time for completing a loss assessment will vary based on the scope of the intrusion and the quantity of data compromised, it is essential to provide interim assessments until the reviewing authority determines that no further actions are warranted.

(U) A cyber damage or loss assessment is different from a security, law enforcement, or inspector general investigation. Rather than focusing on who did what in violation of which regulation, cyber loss assessments use that information as context and background in a more focused examination of the effects caused by the intrusion. They are conducted with the purpose of identifying how the network in question was affected and what information (including but not limited to sources, methods, operations, equipment, facilities, locations, plans, strategies, technologies, or programs) was compromised. The assessments include analysis of the consequences of such exposure.

(U) National level assessments must address both the damage a compromise has inflicted on individual U.S. Government departments and agencies, as well as the broader implications for national security. At the national level, loss assessments are likely to address additional factors such as the impact of loss and compromised information on an adversary's ability to deny or deceive the collection efforts of the U.S. intelligence community and/or to feed false or misleading information to U.S. policymakers.

Benefits of conducting a loss assessment (U)

(U) By highlighting broad vulnerabilities, loss assessments can have far reaching effects on organizational policies and programs. They should contribute to on-going analysis of cyber adversarial capabilities, tradecraft, and intentions. At a minimum, by providing managerial, security, and operational lessons learned, they may help prevent similar disclosures in the future. Additionally, by helping understand how losses occurred, assessments can reduce further waste of U.S. Government resources, lessen the risks to U.S. national security, protect the lives of U.S. citizens and protect intelligence sources.

Loss assessment process/methodology (U)

(U) There are number of steps required for a cyber loss assessment, starting with the recognition that an incident has occurred. While there are clearly some initial and time-dependent steps, portions of the methodology are not inherently linear and could easily (and optimally) be pursued in parallel. The following paragraphs provide an overview of the necessary process and/or methodology to conduct a loss assessment. While each loss assessment will be unique, *Figure 5: Assessment of Loss from Cyber Intrusions* provides exemplar issues to pursue.

How did we know?

(U) As an initial step, it is important to consider how we became aware of an intrusion. This will help isolate the data sets necessary for analysis and establish a baseline of “what we know” about an incident or series of incidents. Again, not all cyber intrusions merit a loss assessment. Organizations should establish criteria to determine whether an in depth loss assessment should be undertaken beyond incident reporting. While a single intrusion might not warrant an assessment, a series of intrusions could meet the necessary criteria. Cross-incident or cumulative assessments could be initiated where a specific incident or series of incidents suggest continued, on-going adversarial operations or offer the chance to develop lessons learned from comparing or aggregating incidents and the associated loss or effects. Subject matter experts are needed to evaluate the affected system to determine if criteria for initiation of a loss assessment are present and/or if other affected systems must be reviewed to enable a comprehensive analysis.

Where did the incident occur?

(U) The affected network or networks need to be identified and their nature or purpose understood. This will enable decision makers to determine what sets of expertise will be needed to examine any loss. A preferred approach for loss assessments would call for a standing response group, with ad-hoc action teams to address specific incidents.

(U) The quality of cyber loss assessments, both from a technical, as well as from a systems impact perspective, depends largely on forensics analysis of the impacted electronic media. It is understood that a complete forensics analysis is necessary to ascertain intruder methodology and to identify what system was compromised as a result of the intrusion. Critical to an effective assessment is immediate and comprehensive access to data.

What was the timeframe of the incident?

(U) The assessment should determine when the attack occurred and how long the incident lasted.

Who was responsible for the incident?

(U) Throughout the assessment, information should be gathered to accurately attribute the source of the attack. While this could be considered a parallel objective to determining loss, attribution of the attacker is critical to gauging the risk caused by a specific compromise.

How did the intruder accomplish the attack?

(U) The assessment must address what tools, tactics and techniques were used and should identify any vulnerabilities in technology, processes, and policies that were exploited. An immediate priority for analysis should be placed on identifying indications of an imminent attack. Analysis of adversarial cyber operations and capabilities, as well as prior reviews and recommendations also should be included (e.g., trends and indicators in cyber threat behavior and activity that might allow opportunities to identify, attribute, disrupt, or otherwise stop the intruder's activities).

Why did the intruder take the action?

(U) Included in the assessment should be analytic conclusions about the adversary's intentions (e.g. motives, strategy, specific targeting, etc.) and whether the intruder might use the compromised information to advance his own research and development or related capabilities and operations.

What type of activity occurred during the intrusion?

(U) The loss assessment should catalogue the information that was compromised and whether the data was exposed, altered, and/or exfiltrated from the network. In addition, analysis of the impact on current and future related programs needs to be incorporated. Any effects on the network, such as denial of service or degradation of service, need to be factored into the overall analysis.

What is the impact of the loss?

(U) The assessment should include an analysis of the overall severity of the loss. It should provide mitigation recommendations based on knowledge of the network and its enterprise architecture and connectivity with other trusted networks. Recommendations on the urgency for further loss assessment activities also should be included along with the likelihood of future incidents of a similar nature and the identification of specific issues needed for follow-on assessment or investigation.

Assessment of Loss from Cyber Intrusions

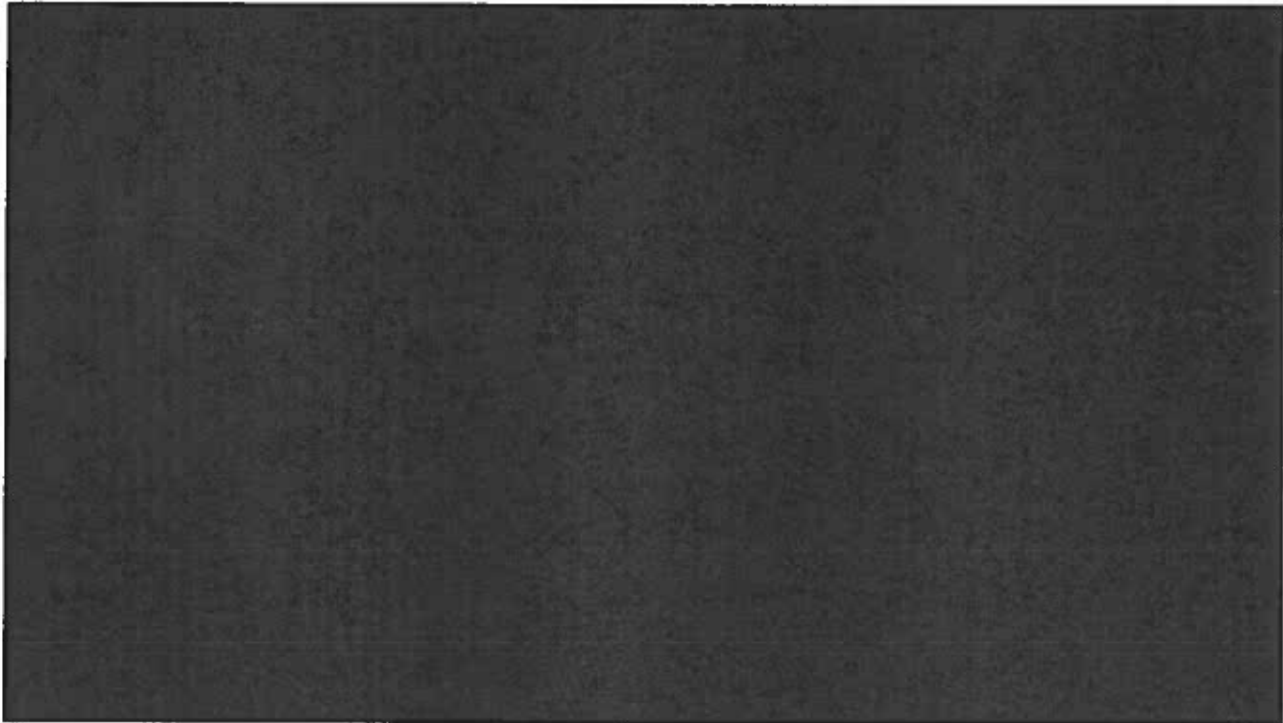


Figure 5: Assessment of Loss from Cyber Intrusions (U//FOUO)

Other Considerations (U)

(U) Loss assessments are unlikely to generate good news for program managers and could consequently be bureaucratically unpopular. It follows that direct, high-level support will be essential to establish and execute this kind of capability. Furthermore, depending on the severity of the loss, program managers may be required to change program direction.

(U) By their very nature, these assessments will expose vulnerabilities and weaknesses and have implications for future operations, planning, and resourcing. Assessment findings and recommendations should be classified and/or compartmented accordingly, consistent with the nature of the networks, operations, and information involved.

Glossary (U)

COMPUTER NETWORK ATTACK (CNA): (S) Actions taken through the use of computer networks to disrupt, deny, degrade, manipulate, or destroy computers, computer networks, or information residing in computers and computer networks. *Source: NSPD-54/HSPD-23.*

COMPUTER NETWORK DEFENSE (CND): (S) Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within U.S. Government information systems and computer networks. *Source: JTF-GNO*

(b)(1)
(b)(3) **COMPUTER NETWORK EXPLOITATION (CNE):** (S) Actions [REDACTED] [REDACTED] conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. *Source: NSPD-54/HSPD-23.*

COUNTERINTELLIGENCE (CI): (U) Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, foreign organizations or persons, or their agents, or international terrorist organizations or activities. *Source: EO 12333*

CYBER COUNTERINTELLIGENCE (Cyber CI): (U) For the purposes of this plan, Cyber Counterintelligence is defined as counterintelligence, by any means, where a significant target or tool of the adversarial activity is a computer, computer network, embedded processor or controller, or the information thereon.

CYBER CI ANALYSIS: (U) The study of the organization, capabilities, intentions, and tradecraft of Foreign Intelligence and Security Services and non-state actors, including foreign terrorist organizations and insider threat activities.

CYBER CI COMMUNITY: (U) Includes all U.S. Government agencies that have cybersecurity and/or counterintelligence missions as defined in The National Counterintelligence Operating Plan (2007). CI Community participants: [REDACTED]

(b)(3)

CYBER INCIDENT: (U) Any attempted or successful access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, an application, or an information system, without lawful authority. *Source: NSPD-54/HSPD-23.*

CYBER THREAT INVESTIGATION: (U) Any actions taken within the United States, consistent with applicable law and presidential guidance, to determine the identity,

location, intent, motivation, capabilities, alliances, funding, or methodologies of one or more cyber threat groups or individuals. *Source: NSPD-54/HSPD-23.*

CYBERSECURITY: (U) Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation. *Source: NSPD-54/HSPD-23.*

CYBERSPACE: (U) The interdependent network of information technology infrastructures, and which includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. *Source: NSPD-54/HSPD-23.*

FEDERAL AGENCIES: (U) Executive agencies as defined in section 105 of Title 5, USC and the U.S. Postal Service (but not GAO). (*Source: NSPD-54/HSPD-23, para h.*) The executive departments in Title 5 include: State, Treasury, Defense, Justice, Interior, Agriculture, Commerce, Labor, HHS, HUD, Transportation, Energy, Education, and Veterans Affairs. We also include contractors and their networks who support these Executive Departments.

INFORMATION SYSTEM: (U) A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. *Source: NSPD-54/HSPD-23.*

INTRUSION: (U) Unauthorized access to a federal government or critical infrastructure network, information system, or application. *Source: NSPD-54/HSPD-23.*

(b)(3)

SECURE: (U) To defend and protect both military and civilian government-owned networks. *Source: NSPD-54/HSPD-23.*

STATE and LOCAL GOVERNMENT: (U) When used in a geographical sense have the meanings ascribed to them in section 2 of the Homeland Security Act of 2002 (section 101 of title 6, United States Code). *Source: NSPD-54/HSPD-23.*

US-CERT: (U) The United States Computer Emergency Readiness Team in the National Cybersecurity Division of the Department of Homeland Security (DHS). *Source: NSPD-54/HSPD-23.*