NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

VULNERABILITY DISCLOSURE FRAMEWORK

FINAL REPORT AND RECOMMENDATIONS BY THE COUNCIL

JANUARY 13, 2004

JOHN T. CHAMBERS
WORKING GROUP CHAIR
CHAIRMAN AND CHIEF EXECUTIVE OFFICER
CISCO SYSTEMS, INCORPORATED

AND

JOHN W. THOMPSON
WORKING GROUP CHAIR
CHAIRMAN AND CHIEF EXECUTIVE OFFICER
SYMANTEC CORPORATION

Acknowledgements

Mr. Chambers and Mr. Thompson wish to acknowledge the enthusiastic support of the entire NIAC Membership in the completion of this effort.

Working Group Members

- John Chambers, President and Chief Executive Officer, Cisco Systems, Inc.
- John Thompson, Chairman and Chief Executive Officer, Symantec Corporation
- Thomas E. Noonan, Chairman , President and CEO, Internet Security Systems, Inc.

Study Group Members:

- Greg Akers, Cisco Systems, Inc.
- Rob Clyde, Symantec Corporation
- Jim Duncan, Cisco Systems, Inc.
- Tara Flanagan, Cisco Systems, Inc.
- Andre Frech, Internet Security Systems and Organization for Internet Safety
- Patrick Gray, Internet Security Systems
- Adam Rak, Symantec Corporation
- Ken Watson, Cisco Systems, Inc.
- Art Wong, Symantec Corporation

Other Study Contributors

- Peter Allor, Information Technology Information Sharing and Analysis Center
- Matt Bishop, Department of Computer Science, University of California, Davis
- Mike Cohen, MITRE Corporation
- Scott Culp, Microsoft and Organization for Internet Safety
- Jack Faherty, DHS-IAIP, MITRE Corporation
- Tom Foster, Financial Services Information Sharing and Analysis Center
- Ernestine Gormsen, Telecom-ISAC

- Shawn Hernan, Computer Emergency Response Team Coordination Center, Carnegie Mellon University

- Rich Pethia, Computer Emergency Response Team Coordination Center Carnegie Mellon University

- Jeffrey Ritter, Kirkpatrick and Lockhart (counsel for the CERT/CC)

- Bruce Schneier, Counterpane Systems

- Paul Vixie, Internet Software Consortium

External Reviewers

- William A. Arbaugh, Department of Computer Science and UMIACS, University of Maryland, College Park, Maryland

- Steven M. Bellovin, AT&T Labs Research

- Matt Blaze, AT&T Labs Research and University of Pennsylvania

- KC Claffy, Cooperative Association for Internet Data Analysis, University of California, San Diego

- Andrew Cormack, UKERNA, United Kingdom

- David Dittrich, University of Washington

- Financial Services ISAC Member Companies

- Wendy Garvin, Cisco Systems, Inc.

- Scott Glasser OPNET Technologies

- Robert Gooch, Cisco Systems, Inc.

- Tiina Havana, Oulu University Secure Programming Group, Department of Electrical and Information Engineering, University of Oulu, Finland

- Paul Hoffman, VPN Consortium

- Lari Huttunen, Oulu University Secure Programming Group, Department of Electrical and Information Engineering, University of Oulu, Finland

- Graham Ingram, AusCERT Information Technology Services, The University of Queensland, Australia

- IT-ISAC Member Companies

- Kathryn Kerr, AusCERT, Information Technology Services, The University of Queensland, Australia

- Marko Laakso, Oulu University Secure Programming Group, Department of Electrical and Information Engineering, University of Oulu, Finland

- Wolfgang Ley, Software Competence Center, Sun Microsystems GmbH, Germany

- Neil Long, OxCERT, Computing Services, University of Oxford, United Kingdom

- Mark Michels, Cisco Systems, Inc.

- David Mortman, Siebel Systems

- Lisa Napier, Cisco Systems, Inc.

- Michael J. O'Connor, Silicon Graphics, Inc.

- Vern Paxson, International Computer Science Institute, and Lawrence Berkeley National Laboratory

- Mike Prosser, Symantec Corporation

- Mike Quinn, Cisco Systems, Inc.

- Damir Rajnovic, Cisco Systems, Inc.

- Juha Roning, Oulu University Secure Programming Group, Department of Electrical and Information Engineering, University of Oulu, Finland

- Derrick Scholl, Sun Microsystems, Inc.

- Telecommunications ISAC Member Companies

Table of Contents

Executive Summary

Introduction. The goal of this report is to achieve a common understanding and develop standard practices for disclosing and managing vulnerabilities in networked information systems. Over the last 20 years, businesses and governments have increased their reliance on networks, applications, and the Internet for core government and business operations. Vulnerabilities in technology vital to interconnected, critical infrastructure operations represent a threat to both national and economic security. Managing these vulnerabilities has become a critical component of customer care and protecting citizens. There are no standards or broad agreements among stakeholders regarding how, when, and to whom to disclose vulnerabilities.

Charter. The National Infrastructure Advisory Council (NIAC) established the Vulnerability Disclosure Working Group (VDWG) in December 2002 to develop the guidelines and recommendations in this report. This framework covers the notification, investigation, disclosure, and resolution of discovered and reported network security vulnerabilities. The guidelines that follow are applicable to all stakeholders in the global vulnerability disclosure process. This report also includes specific recommendations for the President of the United States to direct to the U.S. federal government as appropriate.

Vulnerabilities. Vulnerabilities can be caused by software and hardware design flaws, poor administrative processes, lack of awareness and education, and advancements in the state of the art or improvements to current practices. Regardless of cause, an exploitation of such vulnerabilities may result in real threats to mission-critical information systems. The NIAC recommends the universal use of common naming conventions, such as the example provided by MITRE’s Common Vulnerabilities and Exposures (CVE) project, whenever possible.

Vulnerability life cycle. Every vulnerability is unique, but each evolves through a predictable life cycle. There is a difference between the well-meaning resolution of vulnerabilities and what happens when a malicious actor is involved. The life cycle used in this report assumes a benign environment. The NIAC adopts the following nine-step vulnerability life cycle.

1. Research
2. Verification
3. Report
4. Evaluation
5. Acknowledgement
6. Repair
7. Advisory and patch evaluation
8. Patch release
9. Feedback and case closure

Perspectives. There are numerous schools of thought regarding the disclosure of a vulnerability. At one end of the spectrum are those who believe that vulnerabilities should be publicly announced to compel vendors to develop a patch promptly. Others maintain that information about vulnerabilities should not be disclosed until developers have had a reasonable opportunity to diagnose and offer fully tested patches, workarounds, or other corrective measures. Despite disagreement about when to disclose vulnerabilities, these views share a common goal: reducing the risks to information systems and stopping related malicious activity. Fundamentally, this goal is about protecting not only individual networks and the data that flows through them, but society's use and reliance upon the information highway itself as a fundamental component of commerce and communication around the world.

Stakeholders. Stakeholders may be grouped into four major categories: discoverers, vendors, users, and coordinators. Each major category contains several subgroups, and there are also overlaps between major categories. For example, vendors maintain research staffs that often perform the function of "discoverer." The guidelines in this report have been written for the four primary stakeholder groups.

Scoring. To protect the nation's critical information infrastructure, the Council believes reliable, consistent vulnerability scoring methods are essential. The Study Group evaluated alternative procedures actively employed by several stakeholders to categorize reported vulnerabilities. Existing vulnerability scoring methods vary widely. To protect the nation's critical information infrastructure, the Working Group concluded that reliable, consistent vulnerability scoring methods are essential. Unfortunately, the existing diversity in the methods used to identify vulnerabilities and assign scoring metrics presents a contradictory risk—disagreements provide malicious actors increased time to exploit the vulnerability or increase the damages resulting from existing exploitative situations. Therefore, the NIAC commissioned a research task to develop a consistent scoring methodology. The results of the Scoring Subgroup's work will be published separately when complete.

Communications. Effective vulnerability disclosure depends on effective communication between and among the stakeholders. Vulnerability disclosure has been problematic in the past due to communication issues. E-mail related to managing vulnerabilities should be both encrypted and electronically signed by all participating parties. This ensures the *authentication* and *non-repudiation* of all participants, while preserving the *integrity* and *confidentiality* of message contents. The NIAC strongly endorses the practice of encrypting and signing all E-mail related to vulnerability management as a best practice. Maintaining a trust infrastructure so that people can use public keys easily can be cumbersome, and most encryption products do not interoperate well. PGP (Pretty Good Privacy) and its open-source equivalents like GPG and OpenPGP, are the *lingua franca* of the international incident-response community. Various governments, including the U.S. government, have been slow to adopt PGP or have resisted efforts to use it. As a result, most government agencies have effectively eliminated themselves from the exchange of encrypted communications regarding vulnerabilities. Federal organizations protect sensitive data with Triple-DES and AES-128; both of these algorithms are widely used in secure E-mail programs. Some federal agencies have a clear-text archive requirement for all communication, mandating against the use of encrypted message traffic.

Information Sharing. Existing public and private information-sharing practices were reviewed during this study. Reports of vulnerabilities in software products and services have four primary sources: licensed, authorized users of the products, independent researchers who have been informed by users, discoverers operating at the fringe of commerce, and the vendors themselves. As information sharing is a key component of protecting critical infrastructures, the NIAC strongly endorses the establishment and use of industry Information Sharing and Analysis Centers (ISACs) as vehicles for sharing information on vulnerabilities and their solutions.

However, reports are frequently distributed publicly without any advance verification as to their accuracy. The software vendors and service providers that are the subject of inaccurate reports are distracted from their primary operations and face injuries to their reputation from the reports and related activities. Many of those issuing false reports (a) hide themselves behind anonymous identities, (b) are located outside the United States or (c) are reporting their claims based on the use of unauthorized or "bootleg" copies of the relevant software. As a result, traditional disincentives to false statements, such as defamation lawsuits or criminal investigations, are not available.

Legal Framework. Today, each stakeholder involved in vulnerability disclosure may adopt a differing view regarding the scope and type of role they are willing take. Such decisions are often predicated on the individual stakeholder's assessment of the perceived risk *to them* of incurring financial or other liabilities or reputational injury, or of potentially violating federal or state law. The legal landscape is further complicated by the global nature of vulnerability reporting against a backdrop of conflicting domestic and foreign laws and regulations. Clearly, such variations in both domestic and foreign laws provide an inconsistent foundation from which to manage vulnerability communications and disclosures.

Conclusions. After studying the complex issue of vulnerability disclosure, the NIAC has drawn the following six conclusions:

- Discoverers and vendors often disagree; but not with respect to the fundamental goal to improve the security of software used in critical processes.
- Common terms and procedures are a fundamental requirement for effective vulnerability management.
- Compatible encryption schemes are necessary to ensure all stakeholders can participate in vulnerability management, and to ensure protection of sensitive information.
- A common threat scoring method may help facilitate a foundation for the common understanding among stakeholders.
- Robust information sharing of vulnerabilities, threats, countermeasures, and best practices is key to minimizing threats to critical infrastructure networks.
- Legal and regulatory frameworks at all levels of federal, state, and local government need to be reviewed with the goal of reforming public policy to support the secure sharing of vulnerability information among stakeholders without fear of financial or other liability.

Guidelines. This report includes comprehensive guidelines for all stakeholders in the vulnerability disclosure process. The guidelines are grouped under the major headings of *discoverers*, *vendors*, *end users* and *organizations*, and *coordinators*. Readers are encouraged to read all the guidelines, since some apply to more than one major stakeholder group.

Recommendations. The following seven recommendations are made to the President to direct appropriate Departments and Agencies involved in any aspect of managing software vulnerabilities.

- Support development of a common vulnerability management architecture, including common terms and universally compatible procedures to be employed in the public and private sectors for identifying, reporting, scoring, remediating, and resolving vulnerabilities. This includes standardized E-mail addresses for reporting and standardized Web site locations and content for sharing information effectively.
- Provide policy and funding to ensure that trusted environments are available to protect vulnerability information and ongoing investigations.
- Promote universal use of multiple compatible encryption methods to ensure the U.S. federal government can participate effectively in the global vulnerability management process.
- Conduct a regulatory framework review. The federal government should review existing federal regulations and practices in order to identify barriers to resolving software vulnerabilities.
- Support robust voluntary information sharing through policy and funding. The federal government should set up or support neutral clearinghouses for vulnerability management, accessible to researchers, the private sector, and federal agencies.
- Support a robust infrastructure for international coordination.
- Promote and fund advanced university and industry security research and education.

1. Introduction

Over the last 20 years, businesses and governments have increased productivity, improved efficiency, and created new partnerships by relying on networked operating systems and applications and the Internet. Critical infrastructure operations are now interlinked across sectors, with customers and partners, and with governments at all levels. Governments and businesses have fundamentally changed the way they relate to their citizens and customers—all expect instant availability of key information needed to conduct business. This connectivity is no longer a luxury; it is a *requirement* of core government and business operations.

Vulnerabilities in technology vital to interconnected, critical infrastructure operations represent a threat to both national and economic security. Managing these vulnerabilities has become a critical component of customer care for businesses, and of protecting citizens for governments. Stakeholders in the process—discoverers, vendors, end users, coordinators—all have the same goal: reduce or eliminate software vulnerabilities to ensure continued delivery of critical services and timely, secure flow of information.

How, when, and to whom to disclose vulnerabilities are complex issues. There are no standards or broad agreements among stakeholders regarding vulnerability disclosure. Achieving a common understanding and developing generally standard practices is the goal of this report. Agreement among stakeholders on disclosure practices will improve the expeditious resolution of vulnerabilities, build trust among stakeholders, and help assure delivery of critical infrastructure services to citizens and customers.

Charter

The National Strategy to Secure Cyberspace, published in February 2003, analyzed the issues relating to the disclosure of security vulnerabilities as follows:

> . . . the Nation needs a better-defined approach to the disclosure of vulnerabilities. The issue is complex because exposing vulnerabilities both helps speed the development of solutions and also creates opportunities for would be attackers. In addition, the clearinghouse for such disclosures must be a neutral body between vendors, security companies, and the public at large. Today the government partially funds such organizations. However, the appropriate level and form for this funding need to be reviewed. *DHS will work with the National Infrastructure Advisory Council and private sector organizations to develop an optimal approach and mechanism for vulnerability disclosure.*

The National Infrastructure Advisory Council (NIAC) was formed by Executive Order in October 2002. It is charged with advising the President, through the Secretary of Homeland Security, on information system security issues important to preserving the integrity of the nation's critical infrastructure. The NIAC recognized that a consistent vulnerability disclosure framework could improve vulnerability management and potentially mitigate the risks to information systems, and, to that end, established the NIAC Vulnerability Disclosure Working Group (VDWG), which delivered this report to the Council.

Goal

The NIAC reached consensus that the nation's interests are advanced by a commitment by all stakeholders in cyberspace to responsibly manage, disclose, and resolve vulnerabilities that put the security of the nation's critical infrastructure at risk.

To this end, and in support of the National Strategy, the VDWG set as its goal to develop a framework, built on existing best practices and input from industry and government experts[1], for the notification, investigation, disclosure, and resolution of discovered and reported network security vulnerabilities. The guidelines set forth in this report serve as that framework.

Approach

The co-chairs decided that in order to ensure representation from all major stakeholder groups, including opposing perspectives on the problem, the study group supporting the VDWG should be composed of a cross-section of all those to be represented. During deliberation, the VDWG significantly broadened this representation by soliciting additional input and review by selected, internationally known leaders in each stakeholder community. The following major steps were used in the study of the problem and production of this report:

- Conduct a literature search, including known vulnerability management best practices and white papers on vulnerability disclosure
- Survey study group members and external reviewers to augment the literature search, define the problem, and articulate stakeholder perspectives
- Develop key definitions: vulnerability, vulnerability life cycle, stakeholders; and scope the project: international; guidelines, vice policy; scoring research to be conducted separately
- Write drafts; submit for internal and external review; resolve conflicts in teleconference

See Appendix A for a list of Working Group members, study group members, external reviewers, and resources used to produce this report.

Scope

Security begins with a security policy, which has physical and cyber aspects. Companies, governments, and individuals must make risk decisions governing their critical business operations, processes, relationships, and public access. This report does not cover security policy creation, but is intended to assist readers in managing vulnerabilities that may affect risk. Readers are encouraged to develop fundamental policies on which to make sound risk decisions involving critical infrastructure systems.

Information systems and their hardware and software are produced and consumed all over the world. The Internet is borderless, offering the potential for unlimited global interaction for all connected to it, as well as an interconnected pathway for attacks and other malicious activity. Stakeholders in the vulnerability management process include those that discover them, software vendors, governments, critical infrastructure owners and operators, and other users. Rather than attempt to develop a US-centric policy, the Working Group decided to produce non-binding guidelines with global applicability. Voluntary implementation of these guidelines will help in

[1] See Appendix A for sources of best practices and a list of contributors.

minimizing risk to critical infrastructure systems worldwide, including those important to the United States.

The guidelines that follow will be applicable to all stakeholders in the global vulnerability disclosure process. This report also includes specific recommendations for the President of the United States to direct to the U.S. federal government as appropriate.

Vulnerability Definition

For purposes of this report, a vulnerability is defined as a set of conditions that leads or may lead to an implicit or explicit failure of the confidentiality, integrity, or availability of an information system. Examples of the unauthorized or unexpected effects of a vulnerability may include any of the following:

- Executing commands as another user
- Accessing data in excess of specified or expected permission
- Posing as another user or service within a system
- Causing an abnormal denial of service
- Inadvertently or intentionally destroying data without permission
- Exploiting an encryption implementation weakness that significantly reduces the time or computation required to recover the plaintext from an encrypted message

Common causes of vulnerabilities are design flaws in software and hardware, botched administrative processes, lack of awareness and education in information security, and advancements in the state of the art or improvements to current practices, any of which may result in real threats to mission-critical information systems. Although the presence of a programming flaw is not required, the accidental introduction of defects into software is expected to comprise a significant portion of the vulnerabilities addressed by this framework. The Working Group recommends universal use of common naming conventions such as the example provided by MITRE's Common Vulnerabilities and Exposures (CVE) project, whenever possible.[2]

Vulnerability Life Cycle

Every vulnerability is unique, but each evolves through a predictable life cycle. How do vulnerabilities come to be in the first place? Possibilities include:

- A newly introduced software flaw
- A flaw that has been present since the release of a product
- A fix that reveals a security issue in prior releases of a product, with or without the vendor's awareness
- The result of a complex dependency
- Vulnerabilities introduced into the repository that a vendor uses to distribute code

Figure 1 illustrates the major steps in the life cycle of the resolution of a vulnerability.[3] The continuous arrows in the figure illustrate the major forward steps in the resolution of a

[2] Common Vulnerabilities and Exposures, The MITRE Corporation, http://cve.mitre.org/

[3] Source: Tiina Havana. See full citation in Appendix A.

vulnerability, and dotted lines depict potential paths for feedback or refinement. This life cycle model identifies the "window of vulnerability" as the time between initial discovery to the implementation of a patch or sufficient work-around.

Note that the three columns in the diagram represent different functional groups which may or may not correspond to distinct individuals or organizations. For example, some vendors may employ an internal coordinator—such as a product security response team—with primary duties of coordinating the vendor's vulnerability resolution efforts. In that case the Vendor responsibilities column will also include the Coordinator duties for "Advisory" and "Advisory Release" at the same states as "Repairing" and "Patch Release", respectively. Likewise, note that in some cases, the Discoverer may be the same entity as the Vendor or the Coordinator. Finally, the role of Coordinator is optional.

- **Research:** Discovering vulnerabilities is usually accomplished by research, conducted by security researchers, individuals, coordinators, or vendors themselves. Initial discovery moves a vulnerability from the theoretical realm to something that could be exploited. Some vulnerabilities are discovered by conducting research on actual attacks. All stakeholders conducting vulnerability research should have well-defined root cause analysis processes, with clearly assigned responsibilities for performing this analysis for every attack.
- **Verification:** It is recommended that whoever conducts the research validate the vulnerability by developing a repeatable process to verify its effects and determine possible methods of exploitation.
- **Report:** Communication with affected vendors is the next step in the cycle. This is accomplished either directly or through a coordinator.
- **Evaluation:** Vendors evaluate the reported vulnerability, sometimes working with the discoverer to repeat the conditions under which it was discovered and verify that the exploit reveals a genuine, previously unknown and unpatched vulnerability.
- **Acknowledgement:** Vendors acknowledge receipt of the report, maintaining contact with the discoverer to provide status reports, cooperate in further research, and discuss disclosure plans.
- **Repair:** Vendors develop fixes, typically software patches, for the vulnerability. Sometimes fixes also involve operational procedures or coordination with third-party vendors, especially when the vulnerability affects software on which several vendors' products depend.
- **Advisory and patch evaluation:** Testing validates the effectiveness of the patch, exposes any undesired effects, and may involve subsequent and repeated patch development, especially when the vulnerability affects more than one vendor's product. Ideally, the vendor also tests the patch in multiple environments representing customers' implementations, including testing the patch against many third-party software products normally found in customer networks.
- **Patch release:** Once the vendor is satisfied that the patch is effective and not harmful to most customer software environments, it notifies customers and the general public.

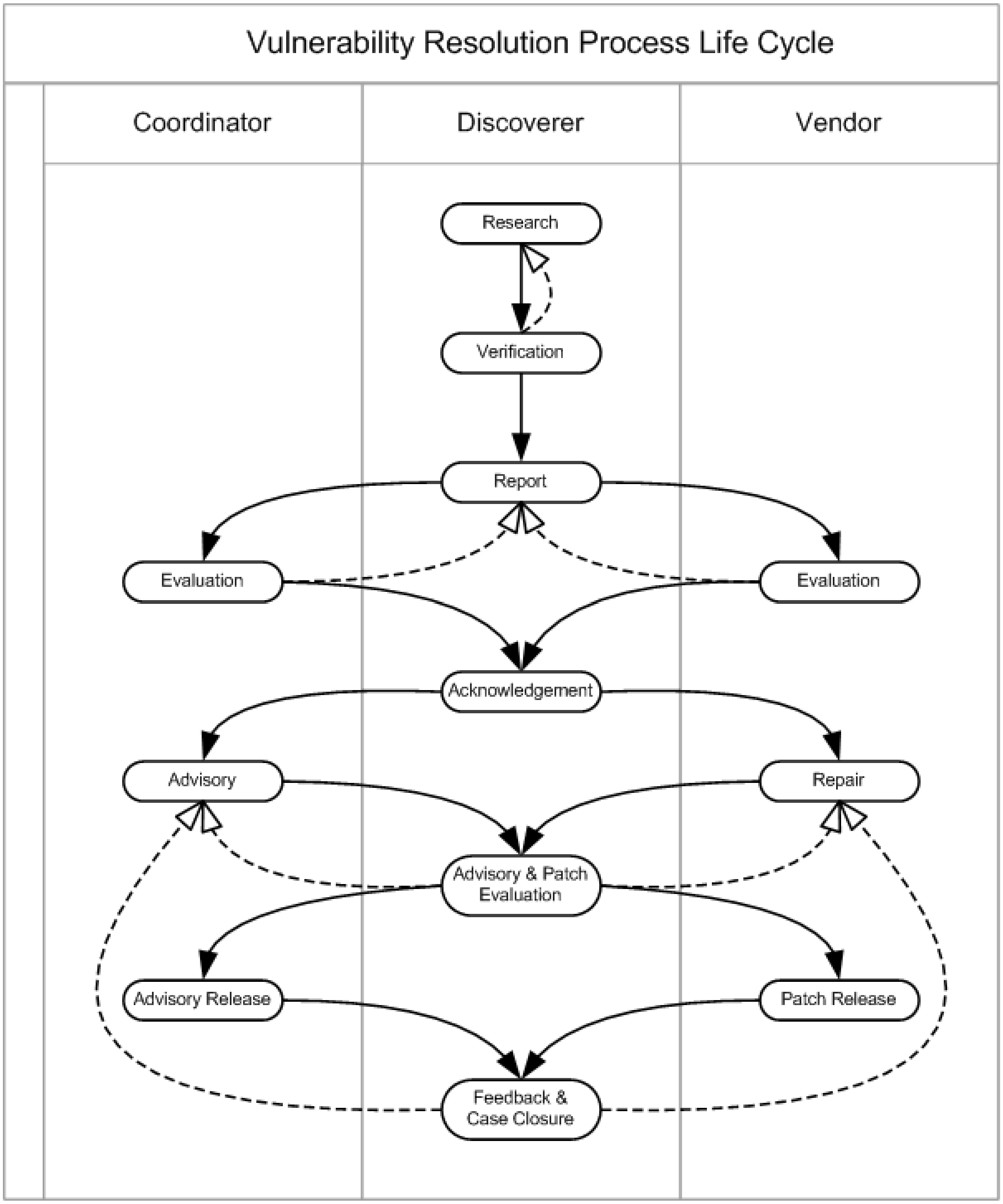

Figure 1: Vulnerability Resolution Process Life Cycle

- **Feedback and case closure:** Any new collateral effects, modifications of the malicious exploit, or new discoveries of the vulnerability or patch's effects on customer installations are fed back to the vendor that issued the patch. The vendor updates advisories as appropriate, generally until further updates are no longer relevant. The reason could be that the vendor has confirmed with a high percentage of customers that affected software is patched; the affected software is obsolete; or the vulnerability and its solution are known for a long time. At this point, the case is considered closed.

Perspectives

There are numerous schools of thought regarding the most appropriate way to minimize the risks associated with the uncontrolled disclosure of a vulnerability. At one end of the spectrum are those who believe that, once discovered, vulnerabilities should be publicly announced so that information system security professionals can begin to mitigate the associated risks and to compel developers to develop a patch to fix the flaw promptly. Proponents of this view contend that those who seek to exploit the flaw are likely to already know about it and informing the public at the earliest possible time may prevent widespread exploitation of that vulnerability.

Others maintain that information about vulnerabilities should not be disclosed to the general public until developers of the affected product have had a reasonable opportunity to diagnose and offer fully tested patches, workarounds, or other corrective measures. Defenders of this latter view claim that limiting the release of information about vulnerabilities reduces the exposure to malicious activity until a fix can be developed and deployed. Despite disagreement about when to disclose vulnerabilities, these views share a common goal: reducing the risks to information systems and stopping related malicious activity.

2. Vulnerability Disclosure Stakeholders

While there are many ways to organize actors in vulnerability disclosure, the study group defined stakeholders in four major categories: discoverers, vendors, users, and coordinators. Each major category contains several subgroups of uniquely interested stakeholders. There are also overlaps between major categories. For example, vendors maintain research staffs that often perform the function of "discoverer." The guidelines in this report have been written for the four primary stakeholder groups. Specific organizations or individuals within these groups should be able to use the guidelines, making any necessary modifications as required by local procedures.

Discoverers

Discoverers include individuals or organizations that find vulnerabilities. Subgroups include researchers, security companies, users, governments, and coordinators.

The vulnerability management process begins with discoverers. Vendors conduct quality assurance testing as part of the development process. Research institutions, security organizations, and interested individuals in both the public and private sectors employ and test software products in creative ways, including some not envisioned by the product vendors. "Hacker" groups are becoming more and more organized, forming clubs and sponsoring conferences, many of which are dedicated to discovering and publishing vulnerabilities in well-known software. Some of these take great pride in being first to publish, regardless of the consequences to the affected vendor or its customers. Others attempt to contact affected vendors directly or through a coordinator, to help the vendor remediate the vulnerability and publish a fix along with the advisory. Typically, the more responsive a vendor is to a responsible discoverer, the less hostile the relationship between discoverer and vendor. In the best of circumstances, discoverers work closely with vendors, sharing test cases and providing sufficient details to enable the vendor to quickly validate the discoverer's claim and focus on remediating the flaw.

Vendors

Vendors develop or maintain information system products or services that may be vulnerable. Subgroups include information security teams, product security teams, incident response teams, researchers, communications coordinators, legal officers, and operators.

In the management of security vulnerabilities, vendors are the key to developing and distributing timely solutions. For the purposes of this document, vendors include both large vendors of software and smaller open-source software development groups. There are primary vendors, who develop a particular technology or product, and secondary vendors, whose products incorporate or rely on another vendors' product. Vendors also include open-source distribution and development repositories, such that it may be impossible to identify a single "vendor" entity. Sometimes a vulnerability is discovered in in-house applications (e.g., Web portals for employees or students, business applications, or other software not intended for sale), or third-party e-commerce infrastructure applications (e.g., Web "carts," billing systems, etc.), which makes identification of the vendor and impact of dependencies on the product very difficult.

Software products created by vendors are the primary targets of malicious exploitation, and vendors are best equipped to design patches and other fixes for their products. However, there is little similarity among software vendors regarding how vulnerabilities are reported, how they resolve them, how they communicate results, and how they work with discoverers, coordinators, law enforcement, and other stakeholders. Inconsistency among vendors can cause confusion among discoverers and the public.

Patches and Workarounds

Vendors develop fixes, typically software patches, for vulnerabilities reported to them. Sometimes fixes also involve operational procedures or coordination with third-party vendors, especially when the vulnerability affects software on which several vendors' products depend. Testing validates the effectiveness of the patch, exposes any undesired effects, and may involve subsequent and repeated patch development, especially when the vulnerability affects more than one vendor's product. Once the vendor(s) are satisfied that the patch is effective and any potential side-effects to customer software environments are understood, they notify customers and the general public.

Most vendors also develop interim workaround solutions that can prevent exploitation in customers' networks until patch development and testing can be completed. This can be especially important when the vulnerability involves software on which vendor products depend, or if patch development is complicated. Discoverers, researchers, and coordinators can assist vendors in developing and communicating workarounds. End users and organizations should implement vendor-published workarounds as operationally feasible, and work with vendors to expeditiously install fully tested patches when they become available.

End Users and Organizations

This group includes everyone using a vendor's product that could be affected by a vulnerability. Subgroups include governments, critical infrastructure owners and operators, and service providers. Each of these groups may also have information security teams, incident response teams, researchers, communications coordinators, legal officers, and operators.

The coordinated effort made by discoverers, vendors, coordinators and others can provide a timely and thoughtful disclosure of information surrounding a vulnerability, intended to mitigate risk to a system. However, in order for the risk represented by a particular vulnerability to be reduced or eliminated, end users and organizations must be notified and must take action to address the problem. Reaching the end users or organizations and their corresponding response to that notification are key components of the disclosure and mitigation process.

Coordinators

Coordinators can manage a single vendor's response or multiple vendors' responses to a vulnerability. Coordinators may also serve as unbiased, independent evaluators of severity, and may act as a medium for communicating with the public and multiple users and vendors. Additionally, coordinators may be able to enhance international reporting, especially in support of organizations that are prohibited from reporting issues to non-citizens. A coordinator may be in a good position to study relationships among vulnerabilities and recognize trends.[4] The most important attribute of a coordinator is to be trusted. Additional attributes required for effective coordination of vulnerabilities include:

- **The ability to reach the correct audience quickly**: One of the main goals of vulnerability disclosure is to motivate system administrators, network managers, policy and decision makers, and others to act in response to a new vulnerability to prevent compromise. To achieve this, vulnerabilities must be disclosed to all affected users, including technical and managerial professionals, as quickly as possible.
- **The ability to marshal experts and decision makers**: Develop solutions in response to new vulnerabilities. Effective vulnerability response requires the ability to gain direct access to senior management, technical officers, scientists, academicians, and policy makers.
- **The ability to communicate securely with stakeholders**: Communications between and among stakeholders must be secure. In the period when a vulnerability is not yet public, message traffic must be strongly encrypted. Without this, the information is at risk of being intercepted, modified, or rerouted in transit. After publication, the public needs to be able to authenticate the veracity of the information. Otherwise, intruders could forge legitimate-looking messages that actually cause system administrators to make their systems less secure. Finally, the cryptographic keys used for these communications must be verifiable and actually be verified by the parties who use them.

[4] See Appendix B for a description of some of these groups.

- **An infrastructure for secure electronic mail**: E-mail related to managing vulnerabilities should be both encrypted and electronically signed by all participating parties.

- **Procedures to guard against information leakage**: It is easy to design secure communication policies that nonetheless leak information about the very topics one is trying to keep secret. Email systems, encryption tools, and communication policies relating to vulnerability disclosure must be carefully considered to guard against unintended information leakage. For example, tools used to encapsulate files and other artifacts into a single unit (e.g., "tar") may also encode information about the machine on which the archiving was performed. Similarly, certain word processor programs may include information in the file that is no longer readily visible and was thought to have been removed.

- **Procedures and tools to compartmentalize information**: It may be appropriate to compartmentalize information between groups. For example, vendors should not necessarily know which of their competitors are vulnerable to a certain problem. Therefore, E-mail messages must be individually signed, encrypted, and delivered directly to each recipient. By contrast, most encryption systems encrypt a single message using multiple keys—one key per recipient. Thus, a traditional system can leak information about everyone the message was sent to, even if the E-mail headers are appropriately constructed.

- **Freedom to inform relevant parties**: The nature and scope of "the next big vulnerability" are hard to predict. An effective vulnerability disclosure process must include the ability to securely inform relevant parties who are only known after initial communication about the vulnerability has occurred. That is, any vulnerability disclosure scheme must include the ability to bring people and organizations "into the loop" prior to public disclosure.

- **A well-known public interface**: The ability to effectively respond to a new vulnerability depends in part on the extent to which an organization is known in the technical circles that discover and respond to new vulnerabilities.[5] Vendors are frequently criticized for the lack of an obvious "front door" for reporting newly discovered vulnerabilities. In some instances, vendors accept reports only if the discoverer has purchased a support contract.

- **Independence**: Newly discovered vulnerabilities often affect multiple vendors, even if the original researcher has identified only a single product during his or her initial research. By reporting his discovery to the vendor prior to public disclosure, the discoverer is acting with the best interests of the public in mind. But what can the vendor do then? Of course, the vendor should fix its own product, but how can this vendor fairly inform other vendors who may suffer from the same or similar vulnerabilities? Large vendors are sometimes inclined to form exclusive organizations in which vulnerability information is shared privately, but where does that leave smaller vendors? A

[5] For example, serious vulnerabilities in LDAP and SNMP were discovered by the OUSPG (University of Oulu [Finland] Secure Programming Group). The OUSPG contacted the CERT/CC in part because the cert@cert.org E-mail address is known worldwide as a vulnerability reporting center.

membership organization may be subject to anti-trust[6] concerns, particularly when information is being exchanged about vulnerabilities in open standards. Stockholders and owners of small and large corporations alike have little interest in expending resources to help their competitors improve their products. Use of a neutral coordinator may be indicated in such instances.

- **A secure infrastructure**: Security begins with physical security, and any organization with stringent data security needs must also carefully guard its physical security.
- **An international reach**: Citizens of one country use software that is produced all over the world. Additionally, compromised computers outside one country present risks to that country's infrastructure. No effective vulnerability disclosure policy can ignore international considerations. This capability should include a 24-hour emergency contact availability.

Stakeholder Subgroups

More details regarding terms used to describe stakeholder subgroups follow:

- **Infosec team**: Staff (individual or group) with the primary responsibility of maintaining and improving information system security for an organization; the infosec team is expected to provide primary response to a vulnerability within the organization.
- **Product security team**: Vendor staff (individual or group) with the primary responsibility of addressing vulnerabilities in the vendor's products on behalf of that vendor.
- **Incident response team (IRT)**: Staff subgroup of an infosec team or product security team charged with handling incidents involving known or emerging vulnerabilities within the parent organization.
- **Incident handler**: An individual or a proxy with primary responsibility for managing an IRT's response to a vulnerability; the incident handler acts as the focal point for communications and direction.
- **Operators**: Administrators, managers, and engineering staff[7] responsible for day-to-day maintenance and improvement of information system resources.
- **Communications coordinators**: Organizational staff responsible for developing or refining messages for recipients at large, such as news media, the public, and internal audiences.
- **Researchers**: Individuals or groups (e.g., information security analysts, validators, testers, historians, intelligence analysts, computer scientists, and paralegal assistants) interested in the reduction of vulnerabilities through technical research leading to countermeasures.

[6] Anti-trust law is known as "competition law" in some other countries.

[7] Commonly called *sysadmins, net admins, system managers*, *operations staff,* or *ops team.*

- **Legal officers**: Individuals responsible for identifying, monitoring and addressing legal issues regarding vulnerabilities. Such issues include liability (product and otherwise), contractual obligations, regulatory requirements (tariffs, export compliance, lawful intercept, and federal or international standards), civil suits or criminal cases (including the serving of papers such as search warrants and subpoenas), and legislative affairs at all levels from local to international law.
- **Law enforcement**: Individuals or groups (e.g., prosecutors and elected or appointed officials at various levels of government[8]) responsible for discovering, appraising, mitigating, or prosecuting violations of the law or threats to national security.

3. Vulnerability Scoring

The study group evaluated alternative procedures actively employed by several stakeholders to categorize reported vulnerabilities. When a vulnerability is first reported, two important steps are performed. First, to help track issues consistently and secure the confidentiality of information relating to the vulnerability, an identification number is assigned. That number is used in all subsequent activities and communications. Second, the vulnerability is scored. The assigned score (also referred to as a “metric”) communicates a sense of the severity of the vulnerability and the importance to be assigned to remediation efforts.

Vulnerability scoring methods vary. The components that are the relevant factors will also vary. Scores assigned to a specific vulnerability may be altered during the course of investigation to reflect the results of investigation or additional developments. For example, confirmed reports indicating the vulnerability has been exploited by malicious actors will result in a significant change in the score; similarly, if the existence of a vulnerability is contradicted by research or if its impact on computer systems is demonstrated to be less significant than reported, a vulnerability score will be lowered.

Vulnerability scores significantly influence the ongoing research, report, and remediation of vulnerabilities. For the purposes of protecting the nation’s critical information infrastructure, the NIAC believes reliable, consistent vulnerability scoring methods are essential. The resulting initial, basic scores will allow resources in both the private and public sectors to better coordinate with each other and to develop locally relevant scores to assist them to prioritize efforts to remediate those vulnerabilities with the greatest potential impact on their own cyberspace-connected assets.

Uniform baseline scoring methods also achieve improved cross-border management of research efforts, particularly those where exploitations of a vulnerability originates outside the United States. Establishing shared meanings regarding a vulnerability involving significant risk will help organize the international assistance that is often essential to the remediation of a vulnerability.

Unfortunately, the existing diversity in the methods used to identify vulnerabilities and assign scoring metrics presents a contradictory risk—to the extent all of the actors adopt different scoring structures, the basis for disagreement arises, which has an impact on how the vulnerability may be resolved. Below a certain score, some stakeholders may elect not to fix a

[8] This group may also include intelligence analysts and individuals such as adjudicators of violations of corporate or organizational policy and third-party arbitrators.

vulnerability when it might be critically important for other specific stakeholder environments. The weaknesses or dangers associated with a vulnerability may be exacerbated by those disagreements, and provide malicious actors increased time to exploit the vulnerability or increase the damages resulting from existing exploitative situations.

Therefore, the NIAC commissioned a research task to develop a consistent scoring methodology. The results of the Scoring Subgroup's work will published separately when complete.

4. Vulnerability Disclosure Communications

Effective vulnerability disclosure depends on good communication between and among the stakeholders. Vulnerability disclosure has been problematic in the past due to communication issues.

Encrypting and Signing

E-mail related to managing vulnerabilities should be both encrypted and electronically signed by all participating parties, whenever possible. This ensures the *authentication* and *non-repudiation* of all participants, while preserving the *integrity* and *confidentiality* of message contents. Open source message formats (such as Open PGP or S/MIME) allow for multiple solutions that are compatible.

However, maintaining a trust infrastructure so that people can easily use public keys can be cumbersome, and most encryption products do not currently interoperate well. Thus, when disparate organizations attempt to use secure electronic mail, they usually choose one of two courses: 1) they attempt to standardize on a single product, which limits the pool of participants, or 2) they attempt to manage the plethora of possible interactions manually. In either case, the high operational cost of sending encrypted mail leads some participants to use other, though more costly, methods to communicate securely or to stop using secure E-mail completely. Still, the NIAC strongly endorses the practice of encrypting and signing all E-mail related to vulnerability management *among known stakeholders* as a best practice.

Encryption. Proper use of encryption preserves the confidentiality and integrity of sensitive information. Only those with proper keys can decrypt the encrypted "cipher-text" into plain-text messages they can use. Encryption provides a reasonable assurance that the message has not fallen into the wrong hands.

Signing. Digital signatures can be used for both encrypted and clear-text messages, and assure recipients of non-repudiation, or that the message is actually from the originator stated in the message.

PGP and Alternatives. PGP and its open-source equivalents like GPG and OpenPGP are the *lingua franca* of the international incident-response community. PGP is used worldwide to encrypt, decrypt, and digitally sign data and messages containing vulnerability information so that it can be shared privately and authentically among response teams, discoverers, and vendors or maintainers. Due to its feature set, ubiquity, open-source nature, and time-to-market, PGP has dominated the field.

Despite PGP's wide adoption among industry, academia, and individuals, various governments, including the U.S. government, have been slow to adopt PGP or have resisted efforts to use it. Many companies also have corporate policies against encrypting E-mail. As a result, some potential stakeholders in the process have effectively eliminated themselves from the exchange of encrypted communications regarding vulnerabilities, or have inadvertently abetted the clear-text sharing of sensitive vulnerability information. In the first case, the government eliminates itself from secure exchange of vulnerability information. In the second case, the use of clear-text increase the risk of compromise of sensitive information.

The actual reasons behind this gap vary greatly. Federal organizations protect sensitive data with Triple-DES (as described in FIPS 46-3) and AES-128 (as described in FIPS 197); both of these algorithms are widely used in secure E-mail programs. Some federal agencies have a clear-text archive requirement for all communication, mandating against the use of encrypted message traffic.

The NIAC does not endorse the use of a specific software application or system to provide the essential service of encrypted, authenticated information sharing. Decreeing the use of a single mechanism is unfair to the developers and vendors of competing, and possibly ultimately superior, solutions, and also places dependence for a key function on a possible single point of failure.

Information Sharing

The most controversial and difficult dimension of vulnerability disclosure is the question of how and when the substance of vulnerability reports (and the related information regarding the investigation, correction, and remediation of verified vulnerabilities) is disclosed and shared with various stakeholders and constituents. The VDWG study group reviewed existing public and private information-sharing practices. Reports of vulnerabilities in software products and services have four primary sources:

- Licensed, authorized users of the products to the software vendor or service provider
- Authorized and unauthorized users inform independent researchers
- Some discoverers who operate at the "fringe" of commerce, acquiring bootleg or unauthorized copies of software applications solely for the purpose of investigating them for vulnerabilities. Not all of these latter actors do so for illegal or improper economic gain; often they are motivated by the desire to contribute to improved security, as well as to establish a successful reputation for identifying vulnerabilities.
- The vendors

Information sharing is a key component of protecting critical infrastructures, and the NIAC strongly endorses the establishment and use of industry ISACs as vehicles for sharing information on vulnerabilities and their solutions.

However, reports are frequently distributed publicly without any advance verification as to their accuracy. Web sites are maintained at which these reports can be transmitted and displayed around the world. Examples are included in the appendix. In some instances, these unverified reports of vulnerabilities are later demonstrated to be inaccurate. The inaccurate reports have many explanations, including the inexperience of the individual publishing the report, who has simply improperly operated the relevant application, or the fact that the vulnerability has already been identified and corrected with a suitable patch. Reports also originate from individuals who have grudges or other complaints regarding the vendor or product in question or from those who seek attention associated with posting a vulnerability claim. There have also been instances of blackmail against vendors.

Inaccurate vulnerability reports are detrimental to the American economy, its businesses, and its citizens. The software vendors and service providers that are the subject of inaccurate reports are often highly distracted from their primary operations and may unjustly suffer injury to their reputation from such false or inaccurate reports and related activities (such as customer inquiries to verify such reports). These businesses are further handicapped by the fact that many of those issuing false reports (a) hide themselves behind anonymous identities, (b) are located outside the United States or (c) are reporting their claims based on the use of unauthorized or "bootleg" copies of the relevant software. As a result, traditional legal disincentives to false statements, such as defamation lawsuits or criminal investigations, are not viable means for legal recourse.

Similarly, vendors must be careful not to deprecate or discount vulnerability reports publicly until they are certain that the report is inaccurate. Many times, early reports of vulnerabilities are incomplete because the reporter does not know what differences exist in the environments of the discoverer and the vendor. A vendor denying a report, only to have it confirmed later, also damages the vendor's reputation, as do vendors who threaten reporters of vulnerabilities with legal action. This further undermines the American economy, its businesses, and its citizens.

Legal and Regulatory Environment

During the life cycle of a vulnerability, each participant faces a series of vital decisions regarding alternative courses of action, which are often influenced by participants' perceptions of their legal environments. In many cases, a stakeholder's participation and management of risks associated with a vulnerability may be at least influence by the likelihood that a particular action or inaction might result in financial or other liability or, at the least, reputational injury for which the law may or may not provide adequate relief. In other instances, stakeholders working to resolve a vulnerability might elect to not execute certain options, or use certain technology tools available in the marketplace, out of their concern that doing so would violate federal or other laws.

The impact of the law on how vulnerabilities are managed and disclosed is further complicated by two additional significant factors:

- First, taking account of the global nature of the manner in which vulnerabilities are reported, many stakeholders outside the United States face different legal and regulatory concerns than those within the United States; as a consequence, their functional roles in working collaboratively with stakeholders in the United States can be influenced by different perspectives on their legal risk. Some stakeholders are global entities with a requirement to comply with multiple nations' laws.

- Second, U.S. federal agencies frequently have vital roles in the resolution of vulnerabilities to federal systems. However, federal regulatory structures and the impact of related federal laws on all stakeholders are inconsistent and incomplete. This unnecessarily complicates the management of vulnerabilities affecting national security.

This report is not a suitable vehicle in which to comprehensively list the various legal and regulatory issues identified by the Study Group; however, the following representative list should be useful in identifying the scope of the task ahead:

- Vulnerabilities are managed through sharing information among various stakeholders, many of whom may have competing products or services in the market. Some stakeholders report concerns that U.S. federal and/or state antitrust or foreign competition laws may inhibit the formation of multi-party organizations through which information can be shared (such as ISACs), or the methods used for disclosure. These concerns have also been raised with respect to coordinators who have contractual arrangements with stakeholders (often their customers or others operating on a subscription basis).

- The Digital Millennium Copyright Act (the "DMCA") prohibits conduct which circumvents, or attempts to circumvent, "access control mechanisms" used to prevent the unauthorized duplication or distribution of copyrighted materials. However, several reporters, researchers and coordinators report that the DMCA limits the scope of research activities that might be conducted with respect to testing and verifying the existence of suspected vulnerabilities.

- In the United States, several federal and state laws have been enacted that directly or indirectly require the development and use of information security practices in connection with different types of services or information assets.
  - Federal laws include the Health Insurance Portability and Accountability Act ("HIPAA") and the implementing regulations that govern the information security for health and patient information; the Gramm-Leach-Bliley Act ("GLB") and the implementing regulations that govern the collection of nonpublic personal information in financial services; the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT"), and the Homeland Security Act of 2002, notably the provisions regulating the disclosure of "critical infrastructure information".
  - States have also been enacting new information security laws, notably California's Information Practices Act (codified at California Civil Code Sections 1798-1798.1), requiring notification of unintentional disclosure of private information, and indirectly encourages the use of encryption for certain types of personal information relating to California residents. Other states have other legislation, often relating to the security with which personal information is held in computer systems. Taken as a whole, these provisions are inconsistent. This inconsistency disrupts the ease with which consistent security protections can be designed into software applications and systems that are victimized by vulnerabilities.

- Taken as whole, these laws and their implementing regulations are complex, broad in scope, and do not offer a framework for the establishment of a consistent reporting process for software vulnerabilities or security protections in software applications and systems.

Today, there is no defined "best practice" with respect to the report of vulnerabilities to vendors across national boundaries. The laws in various countries impose different levels of restrictions on the use of encryption in computer systems and electronic communications. Since encrypted communications among vulnerability stakeholders are viewed as an important strategy for assuring the integrity of information relating to reported vulnerabilities, the variation in foreign laws does not offer a firm foundation from which to proceed in managing vulnerability communications and disclosures. The result is often the exclusion of relevant stakeholders from participating in the cooperative environment that is generally endorsed and encouraged by this report. Vendors usually publish advisories in clear text, and direct communications to known affected customers world wide. A best practice is to clear-sign advisories, but the inconsistency among various national laws governing encryption complicates this, slowing notification to some who need the information.

5. Conclusions

After studying the complex issue of vulnerability disclosure, the NIAC has drawn the following six conclusions:

- Discoverers and vendors alike share the same primary goal of improving the security of software used in critical processes. Vendors and discoverers desire to inform customers and the public of vulnerabilities; their disagreements center on how, when, and to whom to disclose.
- Common terms and processes are a fundamental requirement for effective vulnerability management. Consistent processes for reporting, responding to, protecting, and communicating about vulnerabilities will promote greater understanding among stakeholders. As infection rates of network worms and viruses increase and time between vulnerability announcement and first exploitation shrinks, common understanding and pre-planned procedures become critical to successful threat mitigation.
- Compatible encryption schemes are necessary to ensure all stakeholders can participate in vulnerability management, and to ensure protection of sensitive information.
- A common threat scoring method can provide a potential foundation for common understanding among stakeholders. Knowing the severity or potential impact of a newly discovered vulnerability will assist decision makers to prioritize response and remediation actions.
- Robust information sharing of vulnerabilities, threats, countermeasures, and best practices is key to minimizing threats to critical infrastructure networks.
- Legal and regulatory frameworks at all levels of government need to be reviewed with the goal of reforming public policy to support the secure sharing of vulnerability information among stakeholders without fear of financial or other liability.

www.example.com/security/

- Incident response points of contact
    - Information security team
    - Product security response team
    - Facility or physical security team
    - Copyright and spam abuse contacts, etc.
- Vulnerability management section, including:
    - “How to report”
    - “Latest advisory” section
    - “Hot tips” section
- Links to information on security improvement
    - Recommended best practices
    - Security products

Figure 2: Suggested Content for a “Slash Security” Page

6. Guidelines

These guidelines are designed to eliminate confusion among all stakeholders and the public regarding managing and resolving security vulnerabilities. The guidelines are not to be considered absolute—stakeholders need the flexibility to choose whatever actions are appropriate for their circumstances and environments.

Reporting Mechanism

All stakeholders should adopt a common process for people to report vulnerabilities to them. Discoverers, vendors, governments, researchers, security organizations, and coordinators will all have differing content and purposes for these mechanisms, but consistent mechanisms across stakeholder organizations would greatly simplify and expedite vulnerability management. Each organization should publish their procedures for handling security vulnerabilities so that stakeholders will know in advance how to deal with each other. Probably the most recognized, and most common reporting mechanism is a dedicated E-mail alias, such as the following examples:

- security-alert@example.com
- security@example.com
- secure@example.com
- support@example.com
- info@example.com

Stakeholders’ Web pages should include consistent formats for reporting and displaying security vulnerability information. One suggestion is that public Web sites include a section devoted to security that is easily accessible as a primary domain off the organization’s home page. A subsection would be dedicated to vulnerability management. See Figure 2 for an example.

Contracts and Secure Controls

Where applicable, all stakeholders with the responsibility of potentially sharing vulnerability-related information should adopt the use of contracts and security controls as part of their sharing activities in order to best ensure that the information is disclosed and managed in an appropriate manner. Contract provision would include suitable provisions regarding confidentiality, scope of disclosure, terms regarding how and when the information may be disclosed to others and liability for breach.

Using a universally acceptable non-disclosure agreement (NDA) could help improve the situation, but presents additional issues to be considered. First, agreements between private entities may run afoul of legal requirements to disclose certain vulnerabilities to governments, thus limiting their desirability as information-sharing partners. Second, agreements between government entities may expose information to public disclosure via the U.S. Freedom of Information Act (FOIA) or the equivalent in the states in the United States or other countries. Except where such disclosure is specifically exempted, the latter situation will discourage sharing of information. Third, international cooperation may be more efficient without the liability and legal burdens imposed by an NDA. Finally, NDAs can be problematic for some vendors—most maintain intellectual property rights in patches, and researchers may not always be licensed to receive the patch. NDAs are not always sufficient to ensure intellectual property protection.

Guidelines for Discoverers

Determining the Vulnerability

Typical initial discovery is through vulnerability testing of a software product, by its vendor, a research group, security organization, or interested individual. Some vulnerabilities are discovered by conducting research on actual attacks. All stakeholders conducting vulnerability research should have well-defined root cause analysis processes, with clearly assigned responsibilities for performing this analysis for every attack. Verifying that a test result represents a vulnerability is key to the entire process. Testing must be methodical and repeatable, use full, current versions of the software tested, and utilize methods and tools possibly available in existing, relevant environments. If there have been no prior disclosures of a vulnerability found in a recently superceded software version, and the installed base is large, discoverers should encourage vendors to promote secure upgrades of the old vulnerable version.

Protection of Information

The discoverer must act to protect the information from leaking to external parties between the time of reporting it to the vendor and final public release. This may involve isolating the computer systems involved, preventing access to potentially sensitive information related to the vulnerability on their own system, and encrypting any materials that are at risk of leaking. The discoverer should also protect information in transit when reporting it to vendors or coordinators (encrypting it). Vendors and coordinators must have public keys available to facilitate this.

The discoverer should withhold from any outside party (e.g., the public, peers, acquaintances, forums) any release of exploit code or detailed guide to exploiting the vulnerability when publishing advisories.

Who to Contact

If the vulnerability affects technologies from a single vendor, the discoverer should first attempt to contact that vendor directly. If a large number of systems from different vendors are affected, the discoverer should use the resources of a coordinator to ensure that all potentially affected vendors are contacted.

Many vendors have highly visible and well-known contact points for reporting security issues; unfortunately, many others do not. If the discoverer cannot identify the correct channel for communicating security issues, he or she should contact a coordinator for assistance.

If it is not clear who within a vendor's organization will be handling a vulnerability, the discoverer should not send full technical details unless an initial response has been received.

Vendor Confirmation

Within seven business days of initial contact by the discoverer, the vendor should promptly acknowledge, with a personal response rather than an automated message, that it has received the report. If the vendor does not send a satisfactory acknowledgement, the discoverer should attempt to escalate the issue with the vendor. This seven-day response guideline may need to be accelerated for vulnerabilities exposed by actual attacks, as opposed to theoretical vulnerabilities.

If the discoverer is still unsuccessful, he or she should seek the assistance of a third-party coordinator who may have existing credibility and open channels of communication with the vendor. If a third party can't help, the discoverer must proceed as he or she thinks best. As stated previously, the discoverer should be careful not to provide complete details and should, at first, only seek to facilitate direct contact with the vendor through the coordinator. This seven-day timeline should be established by the vendor, not the discoverer. Some vendors operate in different countries or cultures with different holidays and work schedules that may not be obvious to discoverers. Some software vendors are small businesses that may not be available to respond to all discoverer inquiries immediately. Responsible vendors care about their products and their customers, and should attempt to respond to discoverers in a timely manner.

What Information to Provide

When reporting a security vulnerability to a vendor, the discoverer should provide, via encrypted communication, all technical information and related materials the vendor would need to reproduce the issue. The discoverer should also provide complete revision information, including his or her implementation's current patch level, and a description of the technology's environment (e.g. hardware, configuration, other applications installed, relevant details about the network topology, firewall rules, and anything else that may be of use). The discoverer should provide this information only after receiving acknowledgement from the vendor and knowing with certainty that the information provided is going to the correct group. If the discoverer shares exploit code, the discoverer, vendor, and any involved coordinator should use extreme care to ensure that it is properly labeled and protected.

The discoverer should immediately notify the vendor or coordinator of any new information or errors in the original report.

Conflicting Results on the Validity of the Vulnerability (i.e., vendor cannot reproduce)

If the vendor cannot verify the discoverer’s claims, it may question the credibility of the report. If this happens, the discoverer should try to provide more information or materials for the vendor (e.g., screenshots, stack dumps, debugger output, exploit code, their own affected binary). If this does not suffice, the discoverer should attempt to get corroboration of the issue from a third-party organization with established credibility.

Conflicting Perception of Risk (e.g., vendor says is not a threat)

The discoverer and vendor may disagree about the threat of the vulnerability. The discoverer may insist that the vulnerability is a serious threat while the vendor disagrees. In this situation, a third party (such as a coordinator) should be brought in to assess the risk posed by the issue. Only as a last resort, when all attempts to work with a vendor directly and through a coordinator fail, should a discoverer consider publishing information on a vulnerability for which no fix or workaround exists.

Negotiating a Timeline for Information/Patch Release

The discoverer and the vendor must negotiate a timeline for the release of information and patches. Many times this requires the services of a coordinator. Large vendors are often faced with significant code-base modifications, with numerous builds and regression testing, with several concurrent development versions in process. Some discoverers are not aware of the reasons for these legitimate delays. When developing the timeline, the discoverer needs to consider the vendor’s patch development and testing time, and the vendor should consider the risks of inadvertent disclosure and independent discovery by others.

Vendors sometimes take months to correct security vulnerabilities. The flaw could be a severe design error that requires significant effort to fix. Depending on the severity of the vulnerability and the likelihood of its exploitation, long delays in remediation can result in a prolonged risk to end users.

Publishing Information

When publishing advisories, the discoverer should determine the appropriate amount of technical detail to include. Presenting detailed information about the vulnerability has benefits and risks. If full details are released, it could be easy for fairly unskilled malicious individuals to develop exploits, increasing the immediate risk to end users. However, full details allow system administrators and other users to test the vulnerability for themselves. The discoverer should try to find a balance that will provide sufficient details without unnecessarily jeopardizing users.

During the lifetime of a reported vulnerability, information about the vulnerability may be leaked or released by another individual or group that has discovered the issue independently. If this occurs, the discoverer should coordinate with the affected vendor(s) or a coordinator to assist in the release of a vendor advisory (“forced mode” release), basing the amount of detail on what has been exposed.

Unannounced Fixes

The vendor may fix the vulnerability without issuing an advisory and notifying its users. It is even possible that a vendor may not be aware that they have fixed a security flaw. In this case, since the vulnerability has been fixed, it may be appropriate for the discoverer to publish his or her own advisory on the vulnerability. Before doing so, however, the discoverer should attempt to contact the vendor to request that it issue an advisory or to explain his or her intent regarding publishing any related advisories.

Guidelines for Vendors

Protection of Information

Vendors should develop protection policies and practices, including both physical and information system elements, to isolate vulnerability information, exploit code, and related analysis. This information should be kept confidential and distributed to vendor personnel on a limited basis to those who are tasked to work on solutions and/or develop the public advisories—at least until the phase when the public notification process begins. This isolation includes limiting internal distribution to only those who can bring about solutions. Vendors should also provide for a secure environment for validating and testing vulnerabilities and developing appropriate solutions.

***Rationale**:* Unresolved vulnerability information can be dangerous—to customers and possibly to vendors themselves. If a vendor does not have a firm process for internally protecting unresolved vulnerability information, the risk is greater that such information could be mishandled and become public before solutions are available to protect customers.

Working with Discoverers

If the initial discoverer of a vulnerability is not the vendor, and the discoverer contacts the vendor regarding the issue, the vendor should respond to the discoverer within seven business days from the date of initial contact to acknowledge receipt of the report and provide initial status of response. Vendors should make weekend and holiday schedules information available – perhaps by including it on their "slash security" page—so that a discoverer may determine accurately on which day the initial contact period expires and a response should have been received. In cases of vulnerabilities exposed by actual attacks, the seven-day response time may need to be accelerated.

As resolution proceeds, the vendor should keep the discoverer informed regarding progress, enlisting the discoverer's help as appropriate to recreate the situation demonstrating the security issue. Vendors should publicly acknowledge discoverers in all advisories related to the vulnerability if the discoverer agrees to be recognized. An acknowledgement could be as simple as, *"The issue was reported to [vendor] by [discoverer]."*[9]

Handling Multiple Vulnerabilities Simultaneously

Vendors should establish an augmentation capability, resourced with appropriate skill sets and training, to help existing response teams scale to multiple-vulnerability incidents.

[9] Drawn from Rain Forest Puppy, "Full Disclosure Policy (RFPolicy) v2.0," http://www.wiretrip.net/rfp/policy.html

Rationale: Managing a single vulnerability can be taxing for a vendor. Managing more than one may exhaust a vendor's then-available incident response resources.

Monitoring for Active Exploitation

Vendors should have a contingency plan for urgently disclosing vulnerabilities to customers. Therefore, someone within the vendor's incident response team should have the additional responsibility of monitoring for malicious exploitation.

Rationale: Ideally, vendors are able to develop, test, validate, and distribute fixes to vulnerabilities before their customers are attacked. However, sometimes vendors attempt to publicly exploit vulnerabilities before vendors complete their resolution process.

Liaison with Other Vendors

When they become aware of vulnerabilities, vendors' response teams should proactively warn other vendors of possible hazards to their products. In some cases, especially when a vulnerability affects the products from a great number of vendors, an independent external coordinator may be required.

Rationale: Many vulnerabilities affect more than one vendor. Some affect a protocol that is very widely used, such as the Simple Network Management Protocol (SNMP). Also, software from one vendor is often dependent on software from another, which may in turn be dependent on that of a third. This complex interdependency mandates close relationships among product security response teams. It is in the best interest of all for response teams of vendors to maintain trusted relationships with those of their competitors, partners, and suppliers.

Dealing with Deprecated or Obsolete Software and Hardware

Vendors need a way to retire older products without being compelled by customers who fail to migrate to more current hardware and/or versions of software to fix vulnerabilities on such antiquated software/hardware. However, the vendor's notification for end of life should give customers clear notification when the product will reach its end-of-life status and not be further supported, and ample time during which customers can replace the subject legacy hardware or software. During the interim time period (from announcement that a product will be subject to end of life, and when it actually is at its end of life), the vendor should continue to support the legacy product and fix vulnerabilities.

For any supported product, including products that have been announced for end of life but which have not yet reached the termination date, vulnerabilities should be handled according to the guidelines in this report. However, if a vulnerability is found in software or hardware that has reached its announced end of life, the vendor may elect not to fix or mitigate the problem, but at a minimum should notify customers about the vulnerability and again recommend that they upgrade their product.

Partial vs. Full Notification

Vendors normally attempt to notify all users who may possibly be affected by significant security issues at the same time. This includes customers currently under contract, previous customers, customers not under contract, and customers, developers, and coordinators via an intermediate partner, reseller, or other tertiary relationship. Vendors should provide an avenue for customers to proactively (opt-in) sign up to receive security advisory information from the vendor. Vendors may need to provide additional steps to be taken if there is a perceived threat to a critical infrastructure, although those steps are wholly dependent on the critical infrastructure at risk and the nature of the threat.

Guidelines for End Users and Organizations

Dependencies

End users and organizations should understand the assets on which they depend. Users should conduct surveys and assessments of critical systems to understand, in advance of dealing with a vulnerability, which products, protocols, and technologies they have deployed and what they depend on. No external entity can perfectly assess vulnerability for them, and this understanding will help users react promptly and appropriately when vulnerability information is brought to them.

Support-Level Agreements

It is important that end users or organizations conduct an assessment to determine the appropriate internal resources that will be available in the case of notification of a vulnerability so that the appropriate level of support from the vendor can be obtained. Organizers should designate a point of contact to assist with the coordination and carrying out of a deployment plan with affected internal entities.

***Rationale**:* End users and organizations will often have support-level agreements with vendors to assist in the notification, assessment, and deployment of a fix. The level of the agreement and the corresponding support will vary.

Deployment Plan and Process

The end user and organizations should develop an action plan to deploy fixes for a discovered vulnerability when they are contacted by a vendor about a vulnerability. This plan should include an assessment of systems to verify the existence of that vulnerability, an assessment vehicle to determine the impact of exploitation, a process to obtain the proper fixes from the vendor or other entity, and a plan to evaluate fixes for impact on networks and information systems.

Assignment of Tasks and Workgroup Responsibilities

Once notified of a vulnerability and the corresponding fix, the end users and/or the organizations should assign resources to carry out the deployment and mitigation plan. After notification by vendors, if users fail to take appropriate action, they should bear the consequences.

Protection of Information

End users and organizations should develop and maintain a mechanism for protecting sensitive information regarding vulnerabilities and exploits. If a vendor has provided a patch or other software countermeasure, user organizations need to protect all information regarding the vulnerability until testing proves that the software change creates no unacceptable risk in the user’s network. If a vendor provides advance information on a vulnerability, it is even more critical that users protect that information until the vendor-user-discoverer team can complete the countermeasure testing and installation process.

Disclosure to Public and Customers

The end user or organization should determine if and when it may be necessary to inform its customers when its networks or information systems have been compromised. In some cases this decision will need to be made in consideration of applicable law and the party's contracts. In other instances the organization may want to inform customers about the steps to protect systems or to update them on corrective actions being taken in the case of an incident, such as an ATM system being down. Regardless, a communication plan should be developed and a clear process of communication between the corresponding internal team responsible for vulnerability mitigation and the corporate PR team should exist.

Republishing Advisories; Maintaining Correct Information Downstream

The most authoritative source for information on product vulnerabilities and their solutions is the vendor that maintains the product. Most vendors make every effort to publish advisories as widely as possible, especially ensuring that known customers are made aware of changes expeditiously. It is not possible in all cases to ensure that this "push" approach will keep all affected users informed. If users maintain advisory lists or republish advisories for constituents, it is highly recommended that users check with vendors ("pull") frequently to ensure such information is up to date. Some vendors employ a hybrid "push-pull" notification scheme, "pushing" announcements to their World Wide Web server, but expecting customers to "pull" the information from there.

Guidelines for Coordinators

Awareness

For vulnerability coordination to be effective, vendors and users must be aware of the existence and legitimacy of coordinators. In most cases, this translates to the establishment of a strong "brand" and "brand" recognition. In some cases, particularly when a coordinator has a governance or compliance role, there may be requirements to follow the advice of the coordinator.

Establishment of a Reporting Mechanism

Coordinators should establish a well-known reporting mechanism.

Establishment of a Constituency

Vulnerability coordinators should establish a constituency. For example the Department of Energy's (DOE) Computer Incident Advisory Capability (CIAC) team, whose mission includes acting as a coordinator for the DOE, identifies a constituency in their mission statement[10]:

> The mission of CIAC is to apply cyber security expertise to prevent, detect, react to, and recover from cyber incidents for DOE/NNSA and other national stakeholders.

[10] http://www.ciac.org/ciac/CIAC_vision_mission_stmts.html

Protection of Information

Coordinators should take great care in safeguarding the information in their possession. See other parts of this document.

Handling Multiple Vulnerabilities

Coordinators may be called upon by their constituents and stakeholders to work on multiple vulnerabilities simultaneously. Care must be taken to ensure that multiple streams of work are prioritized correctly according to the goals of the coordinating body, needs of stakeholders, and available resources. Use of the NIAC VDWG scoring methodology could aid in assessing the severity of each vulnerability. Because no two coordinators are likely to have identical goals and priorities, each coordinator may have to evaluate vulnerabilities independently in order to develop a locally correct remediation plan.

Establishing Liaison with Multiple Vendors and Constituents

A coordinator must establish that the individual or organizational unit within a vendor has authority and capacity to make statements regarding the disposition of a vendor's product with respect to any problem report. This is usually not within "ordinary" support channels. A coordinator and vendor must establish a communication channel that both find mutually acceptable.

***Other problems**:* Vendors may have different organizational units that operate along product lines or lines of business, without sharing a common communication infrastructure. This requires the coordinator to be flexible in communication methods.

Negotiating Release Schedules

When coordinators are involved with vendors and discoverers, they should assist in negotiating a release schedule among the stakeholders.

Handling Dependencies

A coordinator may be required to conduct significant research into software, hardware, and firmware dependencies in order to provide complete and correct advice.

***Rationale**:* Vulnerabilities are often discovered in software components on which other software relies. For example, a shared library may be used by dozens or hundreds of products. For instance, vulnerabilities in Microsoft's Internet Explorer often affect other products (including products by third-party vendors) in ways that aren't obvious to end users. Examples of products that are sometimes affected by Internet Explorer vulnerabilities include Lotus Notes, Eudora, and Microsoft Outlook. Furthermore, these dependencies are not typically recorded.

Understanding Aggregate Threat

Vulnerability coordinators may be in a good position to recognize and alert the community to an aggregate threat.

***Rationale**:* Examined separately, the impact of a series of vulnerabilities may appear to be relatively small. However, it is possible that vulnerabilities may "chain" together, so that they present an aggregate threat. These "chained" vulnerabilities may come from disparate products and no single vendor may have control over the set of problems or their solutions. Indeed, it may be the case that examined separately, none of the products involved can be said to be flawed. Only independent third parties can objectively comment on the threat posed by "chained" vulnerabilities and provide unbiased remediation advice.

"Rebroadcasting" Advisories and Maintaining Correct Downstream Content

Coordinators should:

- Validate the authenticity of any alerts considered for rebroadcasting
- Always refer to source material and provide appropriate citations and credit
- Always provide a pointer to vendor-supplied alerts when available
- Recognize their limitations. A coordinator may indeed be a security expert, but no individual or organization can be product experts for all products
- Pay careful attention to quantifiers and modifiers like "may," "should," "some," "any," or "every." Failure to consider quantifiers and modifiers appropriately is a common source of problems.

Rationale*:* Coordinators often repackage alerts produced by other groups into locally preferred formats or in order to provide locally appropriate emphasis. While this can be a valuable service, there are several significant risks when doing this:

- A gullible or inattentive coordinator may provide an inappropriate imprimatur to a bogus alert
- An overly trusting coordinator may accept without criticism the advice of a vendor or other coordinator, thus providing little value added service to their constituents, and allowing a vendor or other coordinator to produce sloppy work
- A coordinator without sufficient understanding of a problem may change the meaning of words provided by a vendor or researcher, and occlude or even change important technical details

These problems may be particularly acute when translating an alert from one language to another.

7. Recommendations for the U.S. President

The following recommendations are made to the President, to direct appropriate Departments and Agencies involved in any aspect of managing software vulnerabilities. Recommendations listed here are intended for the U.S. federal government and may not be appropriate for non-government institutions. They are not in any particular order of precedence.

Support Development of a Common Vulnerability Management Architecture

Direct the federal government to support the development of common terms and universally compatible procedures that must be used in the public sector, and that may be voluntarily used in the private sector, for identifying, reporting, scoring, remediating, and resolving vulnerabilities. Federal departments and agencies should establish common reporting and communications procedures in line with the "reporting mechanism" guidelines in this report. This includes standardized E-mail addresses and Web pages at a well-known location (per each domain name) for reporting and sharing information. In addition:

- Assure establishment of appropriate stakeholder groups in all major federal departments and agencies. Coordinate and assist state governments in establishing these groups and implementing all guidelines in this report.
- Promote the universal use of naming conventions such as MITRE's Common Vulnerability and Exposure (CVE) project to uniquely identify vulnerabilities in a consistent manner.
- Support development and use of a universally compatible vulnerability scoring methodology. When complete, such a scoring method should:
    - Employ standardized threat scoring classification schemes structured around accepted criteria by which to assess and evaluate vulnerabilities. The goal of standardized threat scoring is to promote understanding by a range of private and public sector researchers regarding reported vulnerabilities.
    - Allow for local variations, depending on impact, environment, culture, and roles of those developing scores.
    - Permit ongoing adjustment of an assigned score or set of scores in order to reflect research results or the impact of confirmed exploitations or remediation efforts.
    - Incorporate procedures for independent validation of the suitability of any score or set of scores assigned to a vulnerability, along with a means for improper results to be adjusted in a neutral manner.
    - Enhance existing recognized national and international communication structures through which reported vulnerability information is communicated to qualified stakeholders.

Protect Vulnerability Information and Ongoing Investigations

The federal government should provide policy and funding to ensure that trusted environments are available to:

- Ensure the continuous security and integrity of vulnerability investigations in process and manage the disclosure of related information through secured, trusted mechanisms.
- Protect the confidentiality of vulnerabilities for which no known exploitations have been reported, while affected vendors are working towards a solution.
- Coordinate the voluntary disclosure of information regarding exploited vulnerabilities to take into account, among other factors, the risks of damage to the nation's critical information infrastructure, the need for completion of ongoing investigations, and the coordinated release of suitable solutions or remedies for the vulnerability.

Promote Universal Use of Compatible Encryption

To ensure the U.S. federal government can participate in the global vulnerability management process, it should designate a specific office within each participating agency to review appropriate federal regulations, define guidelines, and act as a clearinghouse to distribute open-source message format standards (such as OpenPGP or S/MIME) that are compatible with current vulnerability management community practices, choose a key validation and distribution system, and provide a profile of which encryption and signature algorithms all federal vulnerability management stakeholders should use. Of course, when a government organization that only allows FIPS-certified encryption is a stakeholder, AES-128 or Triple-DES encrypted communication should be used. An option when none of the above is available would be to use an SSL-encrypted Web site.

Widespread use of compatible encryption would have benefits far beyond vulnerability management. All types of incident information being exchanged within and among ISACs, victims of computer crimes, domestic and international law enforcement, and incident response teams would benefit. This kind of standardized infrastructure is key to improving communications that deal with attacks on critical infrastructures as well as lesser incidents.

Conduct a Regulatory Framework Review

The federal government should review existing federal regulations and practices in order to identify barriers to resolving software vulnerabilities. Barriers to vulnerability resolution include possible penalties for conducting security research and transmitting results to stakeholders, mandatory informing of individuals regarding inadvertent disclosure of their private information, and restrictions on the use of encrypted E-mail for government agencies. This review should also cover various federal civil and criminal laws, including, without limitation, the Digital Millennium Copyright Act (“DMCA”), the Health Insurance Portability and Accountability Act (“HIPAA”), the Gramm-Leach Bliley Act (“GLB”), the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (“USA PATRIOT”), the Homeland Security Act of 2002, the Computer Fraud and Abuse Act, that may directly or indirectly affect the discovery, reporting, disclosure, or protection of sensitive vulnerability information.

This review should also include a survey of related international and state laws. Where applicable, the federal government should assist the States by identifying barriers to effective vulnerability management in State statutes, and should work with other national governments to ensure harmony of international law with the same goals.

Support Robust Voluntary Information Sharing

The federal government should set up or support a neutral clearinghouse for vulnerability management, accessible to researchers, the private sector, and federal agencies. Reporting vulnerabilities to the clearinghouse must be voluntary for any non-government entity. This clearinghouse must be able to conduct secure and trusted research, analysis, remediation support, and disclosure activities, working in close cooperation with the private sector, especially the ISACs, research companies, security vendors, and universities. However, the clearinghouse should not supplant direct communication between a discoverer and a vendor. The NIAC recommends such a clearinghouse as a key node supporting information exchange among industry ISACs and between ISACs and the federal government. The clearinghouse should maintain a meta-database with references to vendor-supported vulnerability databases, along with recommendations for protection of the databases themselves and for their format and content. Specifically, a vulnerability database content might include, for each incident:

- An incident ID
- Each E-mail notification related to it
- Its status in the process
- Methods or tools for determining whether and which systems are vulnerable
- The nature of the damage that could occur
- Countermeasures and instructions for how and when to apply them
- References to external, related material

Support a Robust Infrastructure for International Coordination

Ensure there is a single point of reference for private sector entities and governments to share information, coordinate efforts, and resolve security vulnerabilities. This should include establishment of consistent, secure communications means, working with foreign governments and non-government organizations to spread knowledge of common procedures, collaborating in ongoing investigations, and conducting joint research to improve global vulnerability management.

A second goal of international coordination should be a review of various national laws affecting vulnerability management. This should include a review of laws protecting privacy, restricting communication on vulnerabilities, affecting investigations, and enabling cross-border law enforcement collaboration.

Promote and Fund Advanced University and Industry Security research and Education

The federal government should expand current research funding programs to encourage advanced University and industry research and education into the nature and causes of vulnerabilities, vulnerability management, secure software development, and the coordination and validation of public keys to support an infrastructure for secure electronic mail for all vulnerability management stakeholders.

Appendix A: References

@Stake. 2002 June 05. Security Vulnerability Reporting Policy. Available from http://www.atstake.com/research/policy/ , accessed 2003.

Ross Anderson. 2001. *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley & Sons. ISBN: 0-471-38922-6.

William A. Arbaugh, William L. Fithen, and John McHugh. 2000 December. Windows of Vulnerability: A Case Study Analysis. *IEEE Computer*. Available from http://www.cs.umd.edu/~waa/pubs/Windows_of_Vulnerability.pdf , accessed 2003.

Matt Bishop. 2003. *Computer Security: Art and Science*. Addison-Wesley Professional. ISBN: 0-201-44099-7.

Matt Bishop. 1999 September. Vulnerabilities Analysis. *Proceedings of the Second International Symposium on Recent Advances in Intrusion Detection*. Available from http://nob.cs.ucdavis.edu/~bishop/papers/1999-vulclass/1999-vulclass.pdf , accessed 2003.

Matt Blaze. 2002 September 15 (Preprint, revised 2003 March 02). Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks. *IEEE Security and Privacy* (March/April 2003). Available from http://www.crypto.com/papers/mk.pdf .

Matt Blaze. 2003 January 26. “Keep it secret, stupid!” Posted to *comp.risks* and *Interesting-People*. Available from http://www.crypto.com/papers/kiss.html .

President George W. Bush. 2003 February 28. Executive Order 13286. Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security. *Federal Register* 68, no. 43: 10617-10633. Available from http://www.whitehouse.gov/news/releases/2003/02/20030228-8.html .

California. 2002 September 25. Senate Bill 1386. An act to amend, renumber, and add Section 1798.82 of, and to add Section 1798.29 to, the Civil Code, relating to personal information. Available from http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf , accessed 2003.

Steven M. Christey. 2002 December 27. "Re: Status of draft-christey-wysopal-vuln-disclosure-00.txt". *Internet Engineering Task Force*. Available from http://www.ietf.org/mail-archive/ietf/Current/msg18630.html , accessed 2003.

Steven M. Christey and Chris Wysopal. 2002 February 12 (**Expired 2002 August 12**). Responsible Vulnerability Disclosure Process (Internet-Draft RFC). Available from http://www.vulnwatch.org/papers/draft-christey-wysopal-vuln-disclosure-00.txt , accessed 2003.

Computer Emergency Response Team/Coordination Center. 2000 October 09. CERT/CC Vulnerability Disclosure Policy. Available from http://www.kb.cert.org/vuls/html/disclosure/ , accessed 2003.

Computer Emergency Response Team/Coordination Center. 2003. CERT/CC Vulnerability Metric. Available from http://www.kb.cert.org/vuls/html/fieldhelp#metric .

Russ Cooper. 2001. Proposal – The Responsible Disclosure Forum. Available from http://www.ntbugtraq.com/RDForum.asp , accessed 2003.

D. Crocker. 1997. RFC2142: Mailbox Names for Common Services, Roles and Functions. Available from ftp://ftp.rfc-editor.org/in-notes/rfc2142.txt , accessed 2003.

Electronic Frontier Foundation. 1997-2003. Intellectual Property – Digital Millennium Copyright Act (DMCA) Archive. Available at http://www.eff.org/IP/DRM/DMCA/ , accessed 2003.

Dennis Fisher. 2003 November 18. “Security Researcher Calls for Vulnerability Trade Association.” *eWeek*. Available from http://www.eweek.com/article2/0,4149,1388649,00.asp .

Daniel E. Geer, Jr. (Editor), Dennis Devlin, Jim Duncan, Jeffrey Schiller, and Jane Winn. 2002 Third Quarter. “Vulnerability Disclosure.” *Secure Business Quarterly*. Available from http://www.sbq.com/sbq/vuln_disclosure/ , accessed 2003.

Daniel E. Geer, Jr. (Editor), Mary Ann Davidson, Marc Donner, Lynda McGhie, and Adam Shostack. 2003 Second Quarter. “Patch Management.” *Secure Business Quarterly*. Available from http://www.sbq.com/sbq/patch/ .

Tiina Havana. 2003 April. Communication in the Software Vulnerability Reporting Process. M.A. thesis, University of Jyvaskyla. Full thesis available at http://www.ee.oulu.fi/research/ouspg/protos/sota/reporting/gradu.pdf , brochure available at http://www.ee.oulu.fi/research/ouspg/protos/sota/reporting/brochure.pdf .

Internet Security Systems. 2002 November 18 (Revised). X-Force™ Vulnerability Disclosure Guidelines. Available from http://documents.iss.net/literature/vulnerability_guidelines.pdf , accessed 2003.

Robert Lemos. 2003 June 30. "Law aims to reduce identity theft.” *CNET News.com*. Available from http://news.com.com/2100-1019_3-1022341.html .

Elias Levy. 2001 October 21. “Security in an Open Electronic Society.” *SecurityFocus*. Available from http://www.securityfocus.com/news/270/ , accessed 2003.

Microsoft Corporation. 2002 November (Revised). Microsoft Security Response Center Security Bulletin Severity Rating System. Available from http://www.microsoft.com/technet/security/bulletin/rating.asp , accessed 2003.

Mitre Corporation. Common Vulnerabilities and Exposures. Available from http://cve.mitre.org/ , accessed 2003.

Organization for Internet Safety. 2003 July 28. Guidelines for Security Vulnerability Reporting and Response, Version 1.0. Available from http://www.oisafety.org/reference/process.pdf .

Oulu University Secure Programming Group. 2001 June 28, revised 2003 December 22. Vulnerability Disclosure Publications and Discussion Tracking. Available from http://www.ee.oulu.fi/research/ouspg/sage/disclosure-tracking/ , accessed 2003.

Rain Forest Puppy. Full Disclosure Policy (RFPolicy) v2.0. Available from http://www.wiretrip.net/rfp/policy.html , accessed 2003.

Marcus Ranum. 2000 October. “The Network Police Blotter – Full Disclosure is Bogus.” *;login: The Magazine of USENIX & SAGE*. Volume 25, no. 6: 47-49. Available from http://www.usenix.org/publications/login/2000-10/pdfs/networkpoliceblotter.pdf , accessed 2003.

Mark Rasch. 2003 August 18. “The Sad Tale of a Security Whistleblower". *SecurityFocus*. Available from http://www.securityfocus.com/columnists/179 .

Karl F. Rauscher (Chair, NRIC V Best Practices Subcommittee). 2002 January. NRIC Best Practices. Available from http://www.bell-labs.com/user/krauscher/nric/ , accessed 2003.

Bruce Schneier. 2001 March 15. *Crypto-Gram Newsletter*. Available from http://www.schneier.com/crypto-gram-0103.html , accessed 2003.

Bruce Schneier. 2001 November 15. *Crypto-Gram Newsletter*. Available from http://www.schneier.com/crypto-gram-0111.html , accessed 2003.

Bruce Schneier. 2003 February 15. “Locks and Full Disclosure.” *Crypto-Gram Newsletter*. Available from http://www.schneier.com/crypto-gram-0302.html#1 .

Stanford Law School, Center For Internet and Society. 2003 November 22. Conference on CyberSecurity, Research, and Disclosure. Available from http://cyberlaw.stanford.edu/security/ .

U. S. Copyright Office. 2002 November 19 – 2002 December 18. “Comments on Rulemaking on Exemptions on Anticirumvention.” *Comments on Rulemaking on Anticircumvention*. Available from http://www.copyright.gov/1201/2003/comments/ , accessed 2003.

U. S. Copyright Office. 2003 October 28. "Rulemaking on Exemptions from Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works." *Rulemaking on Anticircumvention*. Available from http://www.copyright.gov/1201/ .

U. S. Department of Homeland Security. 2003 February. *The National Strategy to Secure Cyberspace*. Available from http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf .

U. S. Federal Register. 2003 April 15. Title 6 Code of Federal Regulations Part 29. "Procedures for Handling Critical Infrastructure Information; Proposed Rule." *Federal Register* 68, no. 72: 18523-18529. Available from http://edocket.access.gpo.gov/2003/03-9126.htm .

U. S. General Accounting Office. 2003 February. Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors. *Report to the Committee on Energy and Commerce, House of Representatives*. Available from http://www.gao.gov/new.items/d03233.pdf .

U. S. House. 1998 October 28. *Digital Millennium Copyright Act*. 105th Congress, H.R.2281, became Public Law 105-304. Available from http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=f:publ304.105.pdf , accessed 2003.

U. S. House. 2002 December 17. *E-Government Act of 2002*. 107th Congress, H.R.2458, became Public Law 107-347. Available from http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf , accessed 2003.

U. S. House. 2002 November 25. *Homeland Security Act of 2002*. 107th Congress, H.R.5005, became Public Law 107-296. Available from http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ296.107.pdf , accessed 2003.

U. S. National Institute for Standards and Technology. 1999 October 25. FIPS PUB 46-3. *Data Encryption Standard (DES)*. Available from http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf , accessed 2003.

U. S. National Institute for Standards and Technology. 2003 September 18. FIPS PUB 199. *Standards for Security Categorization of Federal Information and Information Systems*. Available from http://csrc.nist.gov/publications/drafts/draft-fips-pub-199.pdf .

Arne Vidstrom. 2000 September 11. Full Disclosure of Vulnerabilities - Pros/Cons and Fake Arguments. *Help Net Security Staff*. Available from http://www.net-security.org/article.php?id=86 , accessed 2003.

George Will. 2003 February 06. "The FBI's great reformer." *The News & Observer*. Available from http://newsobserver.com/editorials/v-print/story/2174488p-2060299c.html .

Appendix B: Coordinators

Coordinators assist in the disclosure and response to new vulnerabilities. Established in 1988, the CERT Coordination Center (CERT/CC) in Pittsburgh, PA was the first organization to perform this function. In the past fifteen years, the CERT/CC has helped to establish other teams that serve as coordinators for various constituencies, including national teams.

Coordinators serve in four primary capacities:

1. A coordinator acts as mediator and coordinator between disparate vendors affected by the same or similar problems. The primary purpose is to ensure that customers of affected vendors are not placed at undue risk by a competing vendor's announcement. In this role, coordinators serve as a clearinghouse for sharing information between affected vendors prior to public release.
2. Coordinators serve as an independent voice to evaluate the claims of vendors and discoverers. In this role, coordinators provide an unbiased judgment regarding the severity of any particular vulnerability and the efficacy of any particular advice.
3. Coordinators act as a potential, additional medium through which to communicate with the public or local organizations about vulnerabilities and workarounds. A coordinator acting for a small constituency may be in the best position to evaluate threats to that constituency and provide installation-specific advice and guidance. A coordinator acting on behalf of a larger constituency often has the ability to draw a great deal of attention to problems affecting a large number of users.
4. A coordinator is in a good position to study relationships among vulnerabilities and to recognize trends or compounding changes when they occur. For this reason, coordinators may conduct research into the nature and causes of vulnerabilities or may be collocated with leading research groups. In the long term, it is probably this type of activity and relationship that will yield the largest benefit.

Coordinators are typically established for several purposes:

- Research institutions may establish vulnerability coordination activities to support or promote their research agenda and findings. A common subcategory of this type is that a research group may engage in vulnerability coordination for issues it discovers.
- Government organizations may establish vulnerability coordination centers to serve the public interest and protect the critical infrastructure and national security. Vendors and discoverers may choose to notify coordinators, including government computer security incident response teams.
- Commercial organizations may establish vulnerability coordination centers to aid in corporate governance and IT security. In many cases, these organizations have an assessment and compliance role as well. These organizations typically do not provide a coordination service between and among vendors and are usually not involved in predisclosure activity. However, they may serve as the vehicle by which specific corporate security concerns are addressed with software vendors.

- Security solution providers may establish a vulnerability coordination activity as an aid to help ensure their products are up to date.

Legitimization

Coordinators generally do not act with direct authority over a product, and in most cases do not act with legal authority to compel a vendor or discoverer toward any particular behavior. Nonetheless, coordinators achieve their position through a process of legitimization. Like any legitimization process, the legitimization of a coordinator may occur through a variety of means, including demonstrated effectiveness, fiat, precedence, history, and acceptance. Most groups acting as coordinators today have achieved their legitimacy through demonstrated effectiveness, having established a broad audience of system administrators and end users, and by having established productive working relationships with software vendors. In most cases, coordinators have been supported primarily through government funding, and this relationship has aided the legitimization process.

There have been many failed attempts by different groups to become coordinators. There are few active practicing coordinators today. Examples of coordinators are listed at the end of this appendix.

Benefits

Coordinators can bring a variety of benefits to the disclosure process, including:

- Independent evaluation of claims
- Providing comments and criticism to improve a vendor's proposed solution to a new vulnerability
- Investigation and resolution of software dependencies
- Recognizing and minimizing aggregate threat
- Avoidance of allegations of anti-competitive behavior
- Coordination of publication and release schedules to minimize risk
- Management of complex communication issues between and among competing vendors
- Notification to system operators and critical infrastructure groups
- Ability to marshal attention to very serious problems
- Awareness of current events and Internet threats
- Providing anonymization services between vulnerability discoverers and vendors
- Identification of duplicate problems
- Providing information to the public about which products are confirmed not to be affected by a particular vulnerability
- Providing a single point of contact for vendors to work with other vendors
- Providing a single point of contact for discoverers to work with software vendors
- Providing a single point of contact for constituents to address shortcomings in patches and workarounds

Risks

There are two main risks that coordinators present:

1. The risk of unintended disclosure
2. The risk of disclosure adverse to an individual's or organization's position

The first risk is inherent in any information-sharing process. Reputable coordinators should take great care in guarding information to minimize the risk of unintended disclosure, including all the steps discussed elsewhere in this document. But no protections can be absolute; on balance, a responsible coordinator provides benefits for information sharing that outweigh the potential risk of unintended disclosure.

The second risk primarily accrues to intellectual property (IP) holders, though discoverers, especially unscrupulous discoverers, may find risk here as well. A responsible coordinator must have an independent voice with which to advise the community. A coordinator may choose to publicize aspects of a vulnerability that an IP holder would prefer not to be disclosed. Furthermore, a coordinator may choose to release information at a time not of the choosing of the IP holder. Such a scenario is most likely to occur when a vulnerability affects more than one vendor. If one vendor is slow to respond, the coordinator may negotiate a release schedule with the other stakeholders that is adverse to the position of that vendor. In the case of a vendor who shows no evidence that a solution is being pursued, a coordinator may chose to release information about the nature of the flaw and the best-known workarounds.

In many cases, the second risk would be considered a benefit by end users and system administrators.

Invocation

A coordinator may be invoked by any of the participants in the vulnerability disclosure process. Typical scenarios include:

- A discoverer contacting a coordinator prior to public disclosure
- A discoverer contacting a coordinator after encountering an unresponsive vendor
- A vendor contacting a coordinator prior to public disclosure for assistance in alerting the public
- A vendor contacting a coordinator in order to provide competitors with an opportunity to address a vulnerability in the competitor's product.
- An organization asking a coordinator for an evaluation after public disclosure
- A discoverer or vendor contacting a coordinator when a discoverer's issue goes beyond a single vendor's product

Additionally, coordinators may conduct their own investigation in response to public reports if the report is incomplete, inconsistent, or if affected vendors do not appear to have been contacted.

There is no requirement to invoke a coordinator at any stage of the process, though doing so may be helpful.

Reputable coordinators should not act as a hindrance to the safe resolution of a problem regardless of how they are invoked. A coordinator's research agendas and constituent relationships must not interfere with the safe resolution of a vulnerability.

Department of Homeland Security

Information Analysis and Infrastructure Protection Directorate

The federal government agency with primary responsibility for protecting the nation's critical infrastructure and for determining and tracking vulnerabilities to those infrastructures is the Department of Homeland Security, which is comprised of four major directorates: Border and Transportation Security, Emergency Preparedness and Response, Science and Technology, and Information Analysis and Infrastructure Protection. The Information Analysis and Infrastructure Protection directorate analyzes intelligence and information from other agencies (including the CIA, FBI, DIA, and NSA) that involves threats to homeland security and evaluates vulnerabilities in the nation's infrastructure.

National Cyber Security Division

Within the Information Analysis and Infrastructure Protection Directorate, the National Cyber Security Division (NCSD) will provide 24 x 7 functions, including conducting cyberspace analysis, issuing alerts and warning, improving information sharing, responding to major incidents, and aiding in national-level recovery efforts. This division will provide for the federal government's interaction and partnership with industry and other organizations in the cyber security area.

The NCSD will identify, analyze, and reduce cyber threats and vulnerabilities; disseminate threat warning information; coordinate incident response; and provide technical assistance in continuity of operations and recovery planning. The division will coordinate closely with the Office of Management and Budget and the National Institute of Standards and Technology regarding the security of federal systems and will coordinate with federal law enforcement authorities, as appropriate.

NCSD recently formed US-CERT to perform some of these functions. US-CERT is a partnership between NCSD and the CERT/CC.

Information Sharing and Analysis Centers (ISACs)

At the recommendation of the federal government, private industry has organized and begun the operation of various ISACs with the goal of analyzing sector-specific threats and improving information sharing among industry sectors as well as with the government. While there are many models for the structure and working relationships of individual ISACs, the ISACs generally represent the key components of the nation's critical infrastructures. The ISACs generally are composed of industries and government entities that participate in the operation of the critical infrastructures and key national assets. Information of concern to the ISACs includes threats, vulnerabilities, countermeasures, and best practices for security.

CERT Coordination Center

The CERT Coordination Center (CERT/CC) was established by the Defense Advance Research Projects Agency (DARPA) in 1988 following an Internet security incident—the "Morris worm." One of CERT/CC's primary objectives is to analyze the state of Internet security and convey that information to the system administrators, network managers, and others in the Internet community. Staff members also coordinate vendor responses to vulnerability information, informing technology producers, facilitating and tracking their response to the problems, and helping to disseminate solutions. The CERT/CC has proven its ability to keep organizations' identities and other sensitive information confidential, and it is also able to be neutral, enabling staff members to work with commercial competitors and government agencies without bias.

FIRST Teams

The Forum of Incident Response and Security Teams (FIRST) bring together a variety of computer security incident response teams from government, commercial, and academic organizations. FIRST aims to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large. Currently FIRST has more than 100 members. Membership in FIRST enables incident response teams to more effectively respond to security incidents by providing access to best practices, tools, and trusted communication with member teams.

FIRST is an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs.

- FIRST members develop and share technical information, tools, methodologies, processes and best practices
- FIRST encourages and promotes the development of quality security products, policies & services
- FIRST develops and promulgates best computer security practices
- FIRST promotes the creation and expansion of Incident Response teams and membership from organizations from around the world
- FIRST members use their combined knowledge, skills and experience to promote a safer and more secure global electronic environment[11]

FIRST information is available at http://www.first.org/.

Computer Emergency Response Teams (CERTs)

Most countries, states, large government organizations, and enterprises have dedicated CERTs. It is beyond the scope of this report to comprehensively list all existing CERTs. A few examples are provided to show the similarity of mission and wide acceptance of the CERT concept. Many national CERTs are also members of FIRST.

[11] From "FIRST Vision and Mission Statement," www.first.org/about/mission.html, Re-drafted by the FIRST Steering Committee, March 2003, and approved by the FIRST Annual General Meeting, 26 June 2003. Last modified: 7 July 2003.

- The U.S. Department of Defense CERT (DoD-CERT) has the following mission statement: Protects, defends, and restores the integrity and availability of the essential elements and applications of the Global Information Grid (GIG) under the full spectrum of conflict in support of the "Warfighter".[12]
- The Australian CERT (AusCERT) is the national Computer Emergency Response Team for Australia and a leading CERT in the Asia/Pacific region. As a trusted Australian contact within a worldwide network of computer security experts, AusCERT provide computer incident prevention, response and mitigation strategies for members, a national alerting service and an incident reporting scheme.[13]
- UNIRAS is the UK government CERT. On 20 December 1999 the Home Secretary announced the creation of the National Infrastructure Security Co-ordination Centre (NISCC), an interdepartmental organisation set up to co-ordinate and develop existing work within government departments and agencies and organisations in the private sector to defend the CNI against electronic attack. NISCC operates under a Director, who is a member of a Management Board chaired by the Home Office. The other members of the Board are drawn from the Cabinet Office, the Communications-Electronics Security Group (CESG) of GCHQ, the Security Service, the Ministry of Defence and the Police. NISCC's small core staff are from various parent departments contributing to the CNI protection programme. It co-ordinates a programme of work consisting of activity carried out by its core staff, and work carried out under the auspices of various government departments (but contributing directly or indirectly to the overall CNI programme). UNIRAS, the UK Government CERT (Computer Emergency Response Team), is run by NISCC and draws on technical support from CESG, the UK national technical security authority. Its original customers were government departments and agencies. Recently this has been expanded to include: companies holding sensitive government contracts, and most recently CNI organisations. It:
  - Receives reports of significant electronic attack incidents, threats, new vulnerabilities and countermeasures from its customer base and other commercial, government and international sources. It then validates, sanitises (where appropriate) and disseminates the information back to its customers through E-mail alerts and warnings.
  - Provides a helpdesk for its customers, giving advice on IT security incidents, particularly Internet-related problems;
  - Co-ordinates the NISCC's Electronic Attack Response Group (EARG), which responds to serious electronic attack incidents affecting the CNI;
  - Serves as the UK Government CERT (Computer Emergency Response Team) and is an active member of FIRST;
  - Collates reports on IT security incidents supplied by its customers and issues regular statistics. These reports are suitably sanitised to protect commercial or departmental sensitivities.[14]
- CERT POLSKA is the official name of Poland's CERT since January 2001. It was formerly known as CERT NASK. Since February 1997 CERT POLSKA has been a full member of the worldwide Forum of Incident Response and Security Teams. CERT NASK was established in March 1996 according to the disposition of the NASK (Research and Academic Network

[12] www.cert.mil
[13] www.auscert.org.au
[14] www.niscc.gov.uk

in Poland) Director. Current CERT POLSKA headquarters is located at the NASK site in Warsaw, Poland. CERT POLSKA's goals are:

- Providing a single, trusted point of contact in Poland for the NASK customers community and other networks in Poland to deal with network security incidents and their prevention,
- Responding to security incidents in networks connected to NASK and networks connected to other Polish providers reporting of security incidents, and
- Providing security information and warnings of possible attacks cooperation with other incident response teams all over the world.[15]

[15] www.cert.pl

Appendix C: Sample Notification Methods

Notification Method	Description	Management
Public mailing list	A mailing list to which any interested individual may subscribe. The only information sent to this list is advisories, notable updates to advisories, and list management information.	Subscriptions are confirmed through standard mail-back techniques, and addresses from which bounces are received on multiple occasions are pruned. The list itself is maintained within the organization.
Government mailing list	A mailing list composed of other mailing lists managed by DHS/FedCIRC, and to which subscription is limited to authorized individuals.	Subscriptions are administered by DHS/FedCIRC through systems managed by a specific organization.
RSS channel	RSS is an XML-based specification for providing a “Really Simple Syndication” of Web content. RSS content is organized into channels that can be hosted on cooperating Web sites. It can be used to provide links to the most current security alerts.	An RSS channel can be hosted by any Web site that chooses to do so. Readers of that site will see, for example, the ten most recent documents in the channel.
Private notifications of security issues	A signed, clear-text E-mail message notifying authorized users of the existence of a new alert within a restricted database.	E-mail notifications are produced simultaneously with the publication of a new document. The E-mail itself consists only of a pointer to the new document, without disclosing information about the content. The message is signed to guard against various cross-site scripting attacks, and it is delivered individually to authorized readers.

Notification Method	Description	Management
Synopsis of latest vulnerabilities	A signed, clear-text E-mail message consisting of a synopsis of new descriptions of vulnerability published in the database.	The synopses are produced twice a week, covering new entries created during the preceding period. These messages consist of a short synopsis of new vulnerabilities followed by a pointer to additional information. In no case is information sent in clear text that is not publicly available.
Usenet newsgroups	Usenet newsgroups are a popular means of sharing information.	A newsgroup is maintained and managed, and the latest security advisories are posted.
Summaries of recent activity	Quarterly documents summarizing noteworthy new vulnerabilities and intruder activity, delivered to the public mailing list.	Once per calendar quarter, the most noteworthy new vulnerability and incident information is compiled and summarized for subscribers to the mailing list.
Wireless application protocol (WAP) access	Advisories are made available to WAP users, providing mobile users with access to the most critical vulnerability information.	WAP access is managed by the Webmaster or information services team.
Mass media	Regularly conducted interviews with mass media on technical topics.	A media relations office staffed with professional public affairs and media personnel manages requests. Any staff member who interacts with the media should receive professional training.