THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

INTERNET SECURITY/ARCHITECTURE TASK FORCE REPORT

First Steps in Identifying and Remediating Vulnerabilities in Pervasive Software and Protocols

April 4, 2003

TABLE OF CONTENTS

EXECUTIVE SUMMARY

At the President's National Security Telecommunications Advisory Committee (NSTAC) meeting in March 2002, the Special Advisor to the President for Cyberspace Security discussed the challenges of Internet security and the serious nature of the threats posed by vulnerabilities to pervasive protocols within the Internet infrastructure.

In response to these concerns, the NSTAC formed the Internet Security/Architecture Task Force (ISATF) to provide policy recommendations to the President with respect to the vulnerabilities in pervasive software and protocols critical to the operation of the Internet. To accomplish its tasking, the ISATF developed this report, which includes recommendations on the need to improve current information sharing mechanisms so that the telecommunications industry and the Government are better able to quickly and thoroughly respond to and mitigate vulnerabilities before they are maliciously exploited.

The ISATF recognizes that many challenges exist in detecting, mitigating, and correcting vulnerabilities in Internet software and protocols. While industry and Government have taken, and continue to take, major steps to address such problems, perfect system or network security cannot be guaranteed. Consequently, the ISATF feels it is essential that industry and Government effectively and efficiently share information to remain ahead of the threat as much as possible.

The ISATF analyzed five stages relevant to identifying and remediating vulnerabilities in pervasive software and protocols: prevention, detection, information sharing, analysis, and correction. In the area of prevention, the task force advocates aggressive public-private research and development activities and cites the need to develop adequate alerting and warning systems to continue to support the operations of information sharing and analysis centers (ISAC). The task force also identifies barriers to the effective detection of vulnerabilities, such as the myriad number of forums devoted to detection and the lack of standardization in reporting procedures, and offers some solutions, including the establishment of a central Government-sponsored clearinghouse that would serve as a single collection point of interface for the ISACs and other security forums. Thirdly, the task force emphasizes that there are significant barriers to information sharing, such as the Freedom of Information Act (FOIA) and liability concerns, and advocates the creation of legislation that would ease the sharing of critical information. The ISATF also concludes that the analysis functions within industry that detect and publish vulnerabilities appear to be adequate, but Government may find some benefit in better leveraging available synergies by consolidating Government-funded analysis centers where appropriate. Finally, the task force observes that while many organizations are successfully correcting and remediating vulnerabilities, a streamlined method for expeditiously disseminating corrective information to the telecommunications and Internet service provider communities is not utilized. The ISATF believes it would be advantageous to industry if it were able to quickly receive raw data and analysis on vulnerabilities that would allow industry to customize the data analysis to meet its specific services and respond more quickly to incidents.

On the basis of its analysis of issues related to vulnerabilities in pervasive software and protocols, the NSTAC offers the following recommendations:

The NSTAC recommends that the President—

- Consolidate Government-funded watch center operations of agencies and departments dedicated to the detection and dissemination of information related to Internet vulnerabilities into one organization to create a more efficient and effective collaborative industry/Government information sharing partnership, in conjunction with the President's initial recommendation outlined in the National Strategy for Homeland Security;

- Establish a lead organization within the Department of Homeland Security (DHS) to coordinate, with industry, a process for warnings, notification, coordination, and remediation of widespread problems in a national emergency;

- Recognize the need to involve all aspects of the Internet in the process of identifying significant vulnerabilities, including the Web hosting, network access provider (NAP), backbone provider, and Internet service provider (ISP) communities;

- Fund efforts related to identifying and mitigating vulnerabilities in the most critical protocols or software relied on within key sectors of the Nation's infrastructure;

- Direct the DHS, to develop and coordinate with the ISACs, clearly defined government-wide rules for handling and protecting industry-provided critical infrastructure protection (CIP) and vulnerability information;

- Promote and support legislation to address FOIA, antitrust, and liability concerns regarding information shared by industry for the purposes of CIP;

- Develop a process for the Internet community to share information within the component communities and the larger telecommunications and Internet infrastructure context;

- Focus, through a single organization under the DHS, the coordination between critical sectors and serve as the focal point for analysis and dissemination of information regarding the identification and remediation of pervasive software and protocol vulnerabilities; and

- Make Government Information Security Reform Act (GISRA) policies permanent and add requirements that will further enhance its value.

1.0 INTRODUCTION AND CHARGE

At the President's National Security Telecommunications Advisory Committee (NSTAC) meeting in March 2002, the Special Advisor to the President for Cyberspace Security discussed the challenges of Internet security and the serious nature of the threats posed by vulnerabilities to pervasive protocols within the Internet infrastructure.

In response to these concerns, the NSTAC formed the Internet Security/Architecture Task Force (ISATF) to provide policy recommendations to the President with respect to the vulnerabilities in pervasive software and protocols critical to operation of the Internet. To accomplish its tasking, the ISATF developed this report, which includes recommendations on the need to improve current information sharing mechanisms so that the telecommunications industry and the Government are better able to quickly and thoroughly respond to and mitigate vulnerabilities before they are maliciously exploited.

2.0 DISCUSSION

2.1 Prevention

Addressing vulnerabilities in pervasive software and protocols requires a multifaceted approach. A need exists for aggressive public-private research and development activities and for developing adequate alerting and warning systems to support the operations of information sharing and analysis centers (ISAC). Among the capabilities should be the ability to—

- Support infiltration and counterintelligence activities targeted at significant offenders;
- Develop aggressive testing and evaluation programs using raw vulnerability and network management data for modeling, simulation, and automated indications;
- Undertake research and development towards the creation of tools that allow those who exploit vulnerabilities to be tracked or identified more easily; and
- Consider legislative reforms targeted at prosecuting specific people and/or groups who abuse vulnerabilities to launch attacks against U.S. critical infrastructures.

Complicating the need for adequate channels to identify vulnerabilities is the fact that the cost to remediate the problem is staggeringly high. Given that factor, cost becomes the driving factor behind a company's security decisions, and the question of value is paramount. The Government already has a number of policies in place to secure government information technology. Some policies are the result of the Government Information Security Reform Act (GISRA).[1]

[1] For the full text of this act, please see http://thomas.loc.gov/cgi-bin/query/D?c106:1:./temp/~c106y9M6vo:e919845.

As this document is being drafted, GISRA is due to sunset. The Government should make GISRA policies permanent and add needs and objectives that will further enhance its value. The enhancements should include:

- Mandatory baseline security performance standards;
- Independent, third-party assessment and certification;
- Mandatory, explicit linkage to the budget process; and
- Expansion of GISRA-like reporting to identify:
  - Vulnerabilities that involve the private sector as either source or victim;
  - Needs that the reporting agency would like the private sector to address;
  - Collaboration efforts between the reporting agency and other public and private organizations; and
  - Opportunities to expand on the reporting agency's collaboration.

2.2 Detection

Numerous issues compound the detection problem and make the process significantly less effective than it could be. These issues include the following:

- Many forums devoted to increased awareness of Internet vulnerabilities, making it difficult for industry to know where best to focus its efforts;
- An overwhelming volume of intrusion detection data;
- Inadequate resources to process available data and develop appropriate remediation strategies;
- Home users inexperienced in security;
- Unclear and/or differing information sharing needs and objectives;
- Inadequate data mining, correlation, and visualization tools; and
- Duplicate reporting requirements.

In response to Presidential Decision Directive 63 (PDD-63) issued in 1998, the National Coordinating Center for Telecommunications was designated in January 2000 as the Telecommunications Information Sharing and Analysis Center to support the additional information sharing goals outlined in the Administration's National Plan for Critical Infrastructure Assurance.

While the value of information sharing mechanisms has been recognized for many years, the creation of these information exchanges has led to some unintended consequences.

First, there are many forums within industry, Government, and academia devoted to increasing the awareness of Internet vulnerabilities. Many of these bodies engage in duplicative activities that lead to redundant work and information distribution and strain the financial and human resources of both industry and Government.

In addition, the sheer number of information sharing bodies hinders effective communication flows between the groups, instead of facilitating them as expected. Because vulnerability stakeholders are unable to establish trusted relationships with the extensive number of interested parties, communication may become limited and/or non-existent and may lead to the dissemination of confusing or inaccurate vulnerability information.[2] Also, industry and Government may find it difficult to determine which group(s) to consult and when.

A lack of standardization in reporting procedures among the information sharing bodies makes it difficult to effectively share information. It significantly drains the resources of those individuals who are needed to address the vulnerability itself rather than participate in numerous information sharing groups. In addition, the creation of myriad information sharing bodies has narrowed the focus of many groups. As a result, issues may fall "between the cracks" and not be dealt with, which prevents the vulnerability community from efficiently anticipating and reacting to global issues.

A public-private partnership addressing the standardization of information sharing and reporting requirements would assist the detection and reporting process significantly. The formalization of activities would make incident action and escalation quicker and more effective, and would support a dialogue on protecting critical infrastructure and national security. As will be set forth more fully below, a central Government-sponsored clearinghouse should be established. This clearinghouse would serve as a single collection point of interface for the ISACs and other security forums for security-related information, accessible by known and recognized parties. The Government should consider the consolidation of its vulnerability watch desks to centralize information dissemination from disparate Government sources.

2.3 Information Sharing

The NSTAC has previously concluded that there are at least three unresolved impediments to timely information sharing for the purpose of critical infrastructure protection (CIP).[3] These impediments are industry concerns related to the following: 1) Government requirements for disclosure of information under the Freedom of Information Act (FOIA); 2) potential claims related to antitrust concerns; and 3) the liability an enterprise may incur by engaging in the timely sharing of information. Such liability may result from claims brought by one industry enterprise against another for having shared information that involves or implicates that organization. Both parties, industry and Government, must acknowledge that information sharing for the purposes of CIP must be timely yet will often be incomplete and at least partially inaccurate. Legislation should be adopted to remove or limit the liability of an industry enterprise that, in good faith, shares information in a CIP forum established for that purpose.

[2] It is also worth noting that in certain instances, nondisclosure agreements between network operators and vendors may create a legal barrier to disclosing a vulnerability or security concern.

[3] Please reference the Legislative and Regulatory Task Force's March 2002 Report and the June 28, 2001 NSTAC letter to the President for further information.

NSTAC again recommends that the President promote and support legislation to address these three concerns regarding information shared by industry for the purposes of CIP. Such legislation could follow the model used to address the same concerns associated with the year 2000 (Y2K) rollover. Industry and Government broadly supported that legislation.

2.4 Analysis

Cyberspace protection is a shared public-private responsibility. PDD-63 has been the impetus for a significant portion of the work undertaken to date to protect cyberspace. At issue was the lack of a clear source of top-down guidance for this effort. In the absence of leadership, many organizations, both in the public and private sectors, assumed they had a mandate. This view resulted in a fragmented and disjointed approach to vulnerability analysis. Today, when vulnerabilities are detected and published, analysis functions within industry appear to be adequate but they lack the ability to fully capitalize on the available synergies. The Government should recognize that it has a number of organizations/agencies that are involved in duplicative efforts that often fail to complement each other. The Government could better leverage available synergies and enhance information sharing and analysis within the private sector by consolidating analysis centers where appropriate.

The combined capability should be tasked to interface with industry through the clearinghouse described in section 2.2 for the coordination and notification of new vulnerabilities that require specialized infrastructure expertise. The combined Government-funded analysis centers would have the responsibility for bringing together the required parties.

2.5 Correction

Corrections to detected vulnerabilities tend to be appropriately driven through organizations like Carnegie Mellon's Computer Emergency Response Team Coordination Center (CERT/CC), standards bodies such as the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), or through a direct vendor-customer relationship. However, these channels do not ensure that the telecommunications and Internet service provider communities are receiving information in the most timely or effective manner. Additional efforts are necessary to ensure that a public-private partnership can emerge with the intent of identifying key vulnerabilities and remediating them as quickly as possible.

Another prominent problem is the extensive amount of time it takes some organizations to analyze an incident or vulnerability and report back to the stakeholder community due to diluted resources and/or a lack of accountability for not responding faster. In many cases, industry and Government can ill afford to wait for an in-depth report on a specific vulnerability. In addition, many NSTAC companies have noted that quickly receiving the raw data, in addition to any analysis, would allow them to customize the data analysis to meet their specific services and respond more quickly to the incident.[4] Software and hardware manufacturers must be committed

[4] In many instances, access to the test suite identifying the vulnerability is the most critical source of information. Developing a process that can disseminate the test suite with the appropriate level of detail to be of value to the correct communities, while protecting the information from malicious actors, is an important potential function the Government could play. Due to the large number of operating system versions available in network hardware, network operators will develop interim

to driving the anti-vulnerability dialogue. However, the vulnerability identification process is technologically challenging and time consuming. Associated with this process are significant capital and human costs that can be difficult for a single company to bear. The Government can and should encourage the collective benefit of vulnerability identification and remediation by identifying the means by which it can fund or support efforts related to the most critical software or protocols relied upon within key sectors of the Nation's infrastructure. This can include tax incentives, financial support through procurement processes, or direct funding of research and development (R&D) efforts to address the most critical issues first.

The Government can also work with industry to establish best practices in designing corrections that address vulnerabilities in a more holistic approach and explore the use of standards to support the protection of information technology (IT) critical infrastructures. The International Organization for Standardization (ISO) Standard 17799 or the recommendations found within the NSTAC's 1996 *Information Systems Security Board Concept Paper*[5] could provide the basis for developing information security standards within the United States. This approach could be used as an acceptable method of instilling best practices and promoting increased accountability within industry.

3.0 CONCLUSIONS

There are many challenges in detecting, mitigating, and correcting vulnerabilities in Internet software and protocols, including the rapid pace of technological change that renders security tools and solutions effective for only short periods of time. Industry and Government have taken, and continue to take, major steps to address such problems. Industry and Government cannot guarantee perfect system or network security; therefore, it is essential that they effectively and efficiently share information to remain ahead of the threat as much as possible.

The Government should consolidate its own numerous watch center operations and information sharing bodies into one organization that would act as a single "store front" and repository of vulnerability data for industry and Government. Streamlining the Government-funded groups would create a number of benefits for industry and Government, including:

- Reduced redundant activities;
- Reduced reporting requirements;
- Reduced costs for industry and Government;
- Clarity of communications;
- Easier access to more raw data for industry and Government;
- Common formatting and protocols;
- Reduced cycle time from incident detection to report;
- Larger pool of analytical talents and tools applied to the global set of data;
- Better ability to identify global issues;

solutions to protect the network until such time as a more complete solution can be provided by the vendor—access to a test suite is critical during this time period.

[5] To see this full Report, please go to http://www.ncs.gov/nstac/NSVATF%20Report%20(FINAL)_files/ISSBConceptPaper.pdf.

- Development of collaboration and trusted relationships;
- Economies of scale for infrastructure and tool use;
- Better ability for the Administration to engage industry and cybersecurity assets;
- Easier dissemination of best practices; and
- Better ability to analyze collateral impact.

The need for a single Government interface with industry is clear; however, this approach is not without risk. Industry and the Government will need to ensure that trusted relationships already developed in the Internet security realm remain intact during and after the consolidation process. Therefore, for the purposes of CIP, it is the conclusion of this task force that the Government should interface with industry forums (such as the ISACs) from a single Government entity.

4.0 RECOMMENDATIONS

It is NSTAC's position that many issues regarding vulnerabilities in pervasive software and protocols impact telecommunications and Internet service providers. These issues involve many different types of companies and service providers, which are not all related to the provision of telecommunications services. Government funding and support should be considered to encourage under-represented Internet sector providers to participate in the dialogue towards identifying and mitigating vulnerabilities in pervasive software and protocols. Their participation will be absolutely essential towards ensuring that vulnerabilities are identified and addressed across the networks of the Nation. Web hosting companies, network access providers (NAP), backbone operators, Internet service providers (ISP), Voice over Internet Protocol (VoIP) providers, as well as wireless, satellite, and traditional telecommunications carriers all have an interest in understanding the implications of vulnerabilities in pervasive software and protocols. The element common to all these service providers is their reliance on similar vendors —the hardware and software manufacturers—and the ubiquity of certain protocols that are central to operation of the Internet.

These concerns or issues should be coordinated within a single organization that functions as a public-private partnership between industry and the Government, under the auspices of the Department of Homeland Security (DHS). This organization must have the flexibility to allow each sector to address issues relevant to that group in a manner that is reasonable and appropriate to address the vulnerability. With guidance from the DHS, this organization can, in turn, coordinate with other ISACs to share information about ideas for identifying and remediating vulnerabilities in pervasive software and protocols, when appropriate.

To develop a clearinghouse or "single store front" to deal with the identification and remediation of vulnerabilities in pervasive software and protocols, several steps need to occur:

- The clearinghouse should first focus on the protocol and software issues which have the greatest potential impact on the critical infrastructure of the Nation;

- This clearinghouse should be technical in nature and intended solely to address technical concerns related to the identification and remediation of vulnerabilities;

- Critical sectors identified by the DHS should be invited to contribute in a technically substantive manner and be responsible for disseminating information to other members within their respective sector ISACs;

- Participants should identify their trusted sources for working through vulnerability issues in order to develop common sources across ISACs for mitigation purposes;

- The clearinghouse should develop standardized information sharing and reporting processes; and

- This clearinghouse location should include Government sources for vulnerability identification and remediation (i.e., Network Reliability Interoperability Council, National Coordinating Center for Telecommunications Watch and Analysis Operation,[6] Computer Incident Assessment Capability, Federal Computer Incident Response Center, National Infrastructure Protection Center) consolidated under the DHS.

4.1 NSTAC Recommendations to the President

Recommend that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, direct the appropriate departments and agencies, in coordination with industry, to—

- Consolidate Government-funded watch center operations of agencies and departments dedicated to the detection and dissemination of information related to Internet vulnerabilities into one organization to create a more efficient and effective collaborative industry/Government information sharing partnership, in conjunction with his initial recommendation outlined in the National Strategy for Homeland Security;

- Establish a lead organization within the DHS to coordinate, with industry, a process for warnings, notification, coordination, and remediation of widespread problems in a national emergency;

- Recognize the need to involve all aspects of the Internet in the process of identifying significant vulnerabilities, including the Web hosting, NAP, backbone, and ISP communities;

- Fund efforts related to identifying and mitigating vulnerabilities in the most critical protocols or software relied upon within key sectors of the Nation's infrastructure;

- Direct the DHS, to develop and coordinate with the ISACs, clearly defined government-wide rules for handling and protecting industry-provided CIP and vulnerability information;

[6] The NCC Watch is the operational support for the NCC's Telecommunications Infrastructure ISAC. The NCC is a joint industry-Government collaborative body managed by the NCS. As such, its data sources are both industry and Government.

- Promote and support legislation to address FOIA, antitrust, and liability concerns regarding information shared by industry for the purposes of CIP;

- Develop a process for the Internet community to share information within the component communities, and the larger telecommunications and Internet infrastructure context;

- Focus, through a single organization under the DHS, the coordination between critical sectors and serve as the focal point for analysis and dissemination of information regarding the identification and remediation of pervasive software and protocol vulnerabilities; and

- Make GISRA policies permanent and add requirements that will further enhance its value.

APPENDIX A—TASK FORCE MEMBERS, OTHER PARTICIPANTS, AND BRIEFERS

NSTAC MEMBERS

Cisco Systems, Inc.	Mr. Jim Massa, Chair
WorldCom, Inc.	Ms. Joan Grewe, Vice-Chair
AT&T Corporation	Mr. Harry Underhill
Bank of America Corporation	Mr. Roger Callahan
BellSouth Corporation	Mr. Shawn Cochran
The Boeing Company	Mr. Bob Steele
Computer Sciences Corporation	Mr. Guy Copeland
Lockheed Martin Corporation	Mr. Dan Tolley
Lucent Technologies	Mr. David Massarik
Nortel Networks	Dr. Jack Edwards
Northrop Grumman Corporation	Mr. Scott Freber
Raytheon Company	Mr. Jim Craft
Science Applications International Corporation	Mr. Hank Kluepfel
SBC Communications, Inc.	Ms. Rosemary Leffler
VeriSign, Inc.	Mr. Warwick Ford
Verizon Communications, Inc.	Mr. Jim Bean

OTHER PARTICIPANTS

Cisco Systems, Inc.	Mr. Brian O'Connor
George Washington University	Dr. Jack Oslund
Juniper Networks, Inc.	Mr. Pejhan Peymani
Microsoft Corporation	Mr. Sean Finnegan
National Security Council	Mr. Marcus Sachs
Raytheon Company	Mr. Sebastian Taphanel
SBC Communications, Inc.	Mr. Paul Hart
VeriSign, Inc.	Mr. Michael Aisenberg
WorldCom, Inc.	Ms. Cristin Flynn

BRIEFERS

CanSecWest	Mr. Dragos Ruiu
Equinix, Inc.	Mr. Jay Adelson
The Honeynet Project	Mr. Shane Macaulay
National Security Council	Ms. Marjorie Gilbert
Sun Microsystems, Inc.	Mr. Lance Spitzner
University of Washington	Mr. David Dittrich