Global Information Assurance Certification Paper

Tim Casey
GSEC Version 1.4b (amended August 29, 2002)
Option 1 – Research on Topics in Information Security
The National Strategy to Secure Cyberspace: an In-depth Review

Abstract.

The slowdown of the U.S. economy has significantly affected the high-tech and telecommunications industries. Terrorism and war have elevated anxieties and awareness about the need for increased information security. While at first the government is slow to respond with additional resources for cyber defenses, funds will be released eventually. The private IT sector will undoubtedly benefit from these initiatives as they move to assist in carrying out these duties. On February 14th, 2003 the White House released the *National Strategy to Secure Cyberspace*.

The following paper will serve as comprehensive review of the strategy highlighting additional topics for future study. It will provide an insight into this significant national IT security policy from historical, structural, and political standpoints. Government agencies with a role in securing cyberspace are identified along with its proposed private counterparts.

> The way business is transacted, government operates, and national defense is conducted have changed. These activities now rely on an interdependence network of information technology infrastructures called cyberspace. The *National Strategy to Secure Cyberspace* provides a framework for protecting this infrastructure that is essential to our economy, security, and way of life.[1]

The *National Strategy to Secure Cyberspace*[2] is the first national effort to focus on the security of the Internet. It was announced in February 2003 by the President's Critical Infrastructure Protection Board, an entity established by Executive Order 13231 in October 2001.[3] The executive order creating the Board mandated that it "shall recommend policies and coordinate programs for protecting information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems."[4] Despite the clear primary mission of establishing policy on protecting national Information Systems assets, the Board issued two papers: The *National Strategy to Secure Cyberspace* and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*,[5] the latter having originally been included in the *National Strategy for Homeland Security,* released in July of 2002. There was no mention of a need for a cyber protection plan in the July policy paper. Possible reasons for this may include the urgency of a public response to the attack on the World Trade Towers; the unfamiliarity of the Internet in relation to national public policy, especially in terms of cyber security; or the nature of the structure of the Internet in the hands of commercial companies.

Previous attempts to establish a national Information Systems policy can be found in the President's Information Technology Advisory Committee first authorized by the High-Performance Computing Act of 1991 (Public Law 102-194). Still active, the Committee maintains an archive of papers covering topics on integrating technology with health care, education, and taxpayer access to government[6]. Sadly, none cover security. Another example is The Framework for Global Electronic Commerce. Completed in July 1997, it also states the dependency of the economy on what it calls the Global Information Infrastructure. However, security is only presented as a subset of a broader legal issue.[7] President Clinton's May 22, 1998 Presidential Decision Directive 63 (PPD 63) shares much of the structure and content of the current administration's national strategy.[8]

---

[1] Bush, George W. Cover Letter to The *National Strategy to Secure Cyberspace.*
[2] http://www.whitehouse.gov/pcipb/.
[3] http://www.whitehouse.gov/news/releases/2001/10/20011016-12.html.
[4] Executive Order 13231, Section 5; Board Responsibilities.
[5] http://www.whitehouse.gov/pcipb/physical.html.
[6] http://www.ccic.gov/pubs/pitac/index.html.
[7] http://www.ta.doc.gov/digeconomy/framewrk.htm.
[8] http://www.nipc.gov/about/pdd63.htm.

The National Security Council, established by Congress and President Truman in 1947, is another body whose focus excludes cyber-protection despite the mission of providing the President with a "forum for considering national security and foreign policy matters with his senior national security advisors and cabinet officials … the function of the Council has been to advise and assist the President on national security and foreign policies."[9] The National Security Council's presence, with its significant impact on the war on terrorism, can not be found on the White House home page. The direct link is http://www.whitehouse.gov/nsc/. The most significant policy paper by the Bush Administration and the National Security Council is plainly titled the *National Security Strategy of the United States of America*. The paper, as is the Council, focuses squarely on Foreign policy. The paper claims, "Today, the distinction between domestic and foreign affairs is diminishing. In a globalized world, events beyond America's borders have a greater impact inside them,"[10] yet there is no mention of Internet security.

The President's Critical Infrastructure Protection Board, under the leadership of ex-National Security Council Counter-Terrorism expert Richard Clarke, released a *Draft National Strategy to Secure Cyberspace* on September 18th, 2002. Written in very small type and landscape formatted, the 64-page draft was toned down from an earlier, much larger version. It allegedly contained a request to modify the Freedom of Information Act and lift liability provisions for sharing data with the government, according to at least two media sources.[11] The Draft is very straightforward, with an introduction; a section on previous attacks and scenarios; and five "levels," based on the intended audience. The levels are,

1. Home User and Small Business
2. Large Enterprises
3. Critical Sectors (Federal Government, State and Local Government, Higher Education, Private Sector)
4. National Priorities
5. Global

Each level was followed by a grid accompanied by its own recommendations, programs, and discussions designated by a number. For example, R4-1 is for the first recommendation of Level 4. Readers will find the Programs section very useful in identifying existing programs and websites related to the topic. The largest of the levels, with 49 recommendations and 28 discussion points, is number 4: National Priorities. The main purpose of the Draft was to solicit additional feedback for the final policy. The public was directed to the site: http://www.securecyberspace.gov for a chance to submit comment. As

[9] http://www.whitehouse.gov/nsc/.
[10] *The National Security Strategy,* p.31.
[11] http://www.eweek.com/article2/0,3959,547303,00.asp.
http://news.com.com/2100-1023-958545.html#.

of this writing, securecyberspace.gov redirects to http://www.whitehouse.gov/pcipb/, home of the final draft. The Draft is missing, as well as any of the public comments, although the Draft is available elsewhere.[12] An interesting future topic would be the analysis of the feedback.

Reaction to the draft was varied. Some say it was too laissez-faire. Typical of Republican approach to government, the policy statement demanded voluntary cooperation. Much of this "public-private partnership" language survived into the final version. Good security practice says education is half of the battle, but if procedures cannot be carried out to completion or verified, how good is it? Then again, is it practical to have one policy that covers the global Internet?

The *National Strategy to Secure Cyberspace* has fewer pages than the draft, is written in a larger typeface, and reads in two columns instead of three. It can be thought of as three separate documents, each containing similar content. The first section, the Executive Summary, consisting of seven pages, is a very high level overview of each of the Strategy's priorities with numbered lists of action items from each. (The priorities will be discussed in more detail below.) The Executive Summary is followed by an introduction. Much of the exact text from the Executive Summary appears in the introduction, which at first makes one wonder if the page was accidentally turned back or if there is a typo. The introduction has the same priority points as the Executive Summary, but without the numbered action items. Two smaller sections, "Cyberspace Threats and Vulnerabilities" and "National Policy and Guiding Principles," follow the introduction. The former section paints the picture of previous attacks such as NIMDA and Code Red while at the same time forecasting possible future attacks. It also includes the five levels found in the draft, but matches them against the priorities in the form an XY grid. The latter section contains a high-level national policy statement, which is prudent and concise. Guiding principles follow and are written clearly. The Department of Homeland Security[13] was established during the time the final draft was being finalized; perhaps another reason the National Strategy document was delayed. The introduction, and the following two sections can be thought of as the second document. The last document alone, the heart of the *National Strategy to Secure Cyberspace,* contains an adequate level of detail. It consists of five sections each devoted to a separate national priority. They are:

1. A National Cyberspace Security Response System
2. A National Cyberspace Security Threat and Vulnerability Reduction Program
3. A National Cyberspace Security Awareness and Training Program
4. Securing Government's Cyberspace

[12] http://www.pcworld.com/downloads/file_description/0,fid,22329,00.asp.
[13] http://www.dhs.gov/dhspublic/.

5. National Security and International Cyberspace Security Cooperation

Nowhere in the strategy does it suggest that one priority has urgency over another, despite the numerical order in which they are placed. The priorities are matched in the form of a table against the list of levels, first revealed in the draft.[14] (See Table 1.) The levels are a main element of the draft, but in the final version they exist as a subcategory of a section named Awareness in Priority III. It appears the table was added to the final edition as an afterthought or simply as a sop to the draft.

Roles and Responsibilities in Securing Cyberspace					
	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5
	National Cyberspace Security Response System	National Cyberspace Security Threat and Vulnerability Reduction System	National Cyberspace Security Awareness and Training Program	Securing Governments' Cyberspace	National Security and International Cyberspace Security Cooperation
Home User/Small Business		X	X		
Large Enterprise	X	X	X	X	X
Critical Sectors/ Infrastructure	X	X	X	X	X
National Issues and Vulnerabilities	X	X	X	X	
Global					X

Table 1

The guiding principles of the strategy can be summarized into the following themes: 1) A national effort to collaborate and share information about threats and to each do one's part in securing one's own systems. 2) Protection of privacy and civil liberties. 3) Strategy being driven by market forces, not government regulations. 4) Accountability and responsibilities, in the form of an agency list and descriptions of respective areas of focus. 5) Flexibility in planning and execution of response systems. 6) Multi-year effort including ongoing revisions.

While the Department of Homeland Security gets the bulk of the responsibility in executing the strategy, the Office of Management and Budget is listed as the agency, which "oversees the implementation of government wide policies, principles, standards, and guidelines for federal government computer

[14] *National Strategy to Secure Cyberspace,* p.9.

security programs."[15] Each Cabinet level agency is listed in a table along with the commercial and government industry sectors they lead in relation to the strategy.[16] (See Table 2.) The body of the strategy along with future real-world actions will be judged by whether or not the principles are met and how each agency performs.

CRITICAL INFRASTRUCTURE LEAD AGENCIES	
LEAD AGENCY	SECTORS
Department of Homeland Security	• Information and Telecommunications • Transportation (aviation, rail, mass transit, waterborne commerce, pipelines, and highways (including trucking and intelligent transportation systems) • Postal and Shipping • Emergency Services • Continuity of Government
Department of the Treasury	• Banking and Finance
Department of Health and Human Resources	• Public Health (including prevention, surveillance, laboratory services, and personal health services) • Food (all except for meat and poultry)
Department of Energy	• Energy (electric power, oil and gas production, and storage
Environmental Protection Agency	• Water • Chemical Industry and Hazardous Materials
Department of Agriculture	• Agriculture • Food (meat and poultry)
Department of Defense	• Defense Industrial Base

Table 2

Priority I of the strategy is to build a National Cyberspace Security Response System. This is likened to the national radar missile defense system established in the 1950's and 60's. According to interviews with Richard Clarke, part of such a system would be analogous to the network control systems found in major telecommunications companies.[17] These companies have vast rooms with indicators of major outages. Such sharing mechanisms are dubbed Information Sharing and Analysis Centers or ISACs. Richard Clarke is credited with establishing several ISACs. They are industry sector-driven, limited liability companies. For example, there is an ISAC for financial institutions, a separate

[15] *National Strategy to Secure Cyberspace,* p.17.
[16] *National Strategy to Secure Cyberspace,* p.16.
[17] http://www.techtv.com/screensavers/story/0,24330,3374341,00.html.

ISAC for electric utility companies, and so on. The idea is that if one member is hit by an attack, it can communicate to the others within its ISAC. The attacked member would submit its information anonymously so as not to gain a disadvantage against its competitors. (Is it possible these sharing entities violate any 20th century antitrust laws?) The ISACs would tie into a Department of Homeland Security Incident Operations Center that would monitor warnings. It should be noted, however, that many ISACs were formed soon after President Clinton's Presidential Decision Directives 62 and 63, which established the position of National Coordinator for Security, Infrastructure Protection and Counter-Terrorism.

Several of the current ISACs have a web presence with their own style of authentication, online membership subscription, and incident reporting mechanisms. The Financial Systems-ISAC[18] lists board members from Goldman Sachs, Fannie Mae, and NASDAQ. Their site functions as a marketing tool with no current listing of vulnerabilities and no way to log in. To join, one has to mail a signed application in return for authentication and login instructions. A curious observation: the Financial Systems-ISAC does not share any data with the government. From the site's FAQ, "Does the US Government have access to FS?ISAC [sic] reports? No. US Government agencies, such as NIPC, submit information but cannot access data."[19] Other industry ISACs include the Electricity Sector,[20] Water,[21] Surface Transportation,[22] and Information Technology.[23] IT-ISAC maintains a list of the major security vulnerabilities and is backed by industry heavyweights such as Cisco, HP, Microsoft, Oracle, and others.

The National Cyberspace Security Response System should be thought of as a process broken down into four general areas: Analysis, Warning, Incident Management, and Response/Recovery. The first area, Analysis, will consist of vulnerability assessments and general research. During the Warning phase, ISACs are supposed to connect to the Department of Homeland Security Operations Center via a secure Cyber Warning and Information Network (CWIN). CWIN was first envisioned as an "out-of-band" or separate mechanism to contact key agencies in case the entire Internet became unusable.

Incident Management involves responding to an event reported through the ISACs and CWIN to the Department of Homeland Security. It thus requires such a CWIN to be established. As of this writing, it is not clear any progress has been made toward this effort. However, voluntary sharing with the Department of Homeland Security has already begun, as illustrated with the recent Sendmail

[18] http://www.fsisac.com/index.cfm
[19] http://www.fsisac.com/faq.cfm
[20] http://www.esisac.com/
[21] http://www.waterisac.org/
[22] http://www.surfacetransportationisac.org/
[23] https://www.it-isac.org/

vulnerability.[24] Information Security Systems[25] (ISS), an intrusion detection and security company, notified the government about the vulnerability. The government then worked with Sendmail and other vendors to secure government computers first. This method has met with criticism from advocates of more open bug tracking and notification processes.

Finally, Response and Recovery covers such areas as business continuity planning, disaster recovery planning, risk assessments, etc. Lead government agencies are instructed to "encourage" their private industry counterparts to develop contingency plans. The strategy should be credited for including these crucial aspects of security.

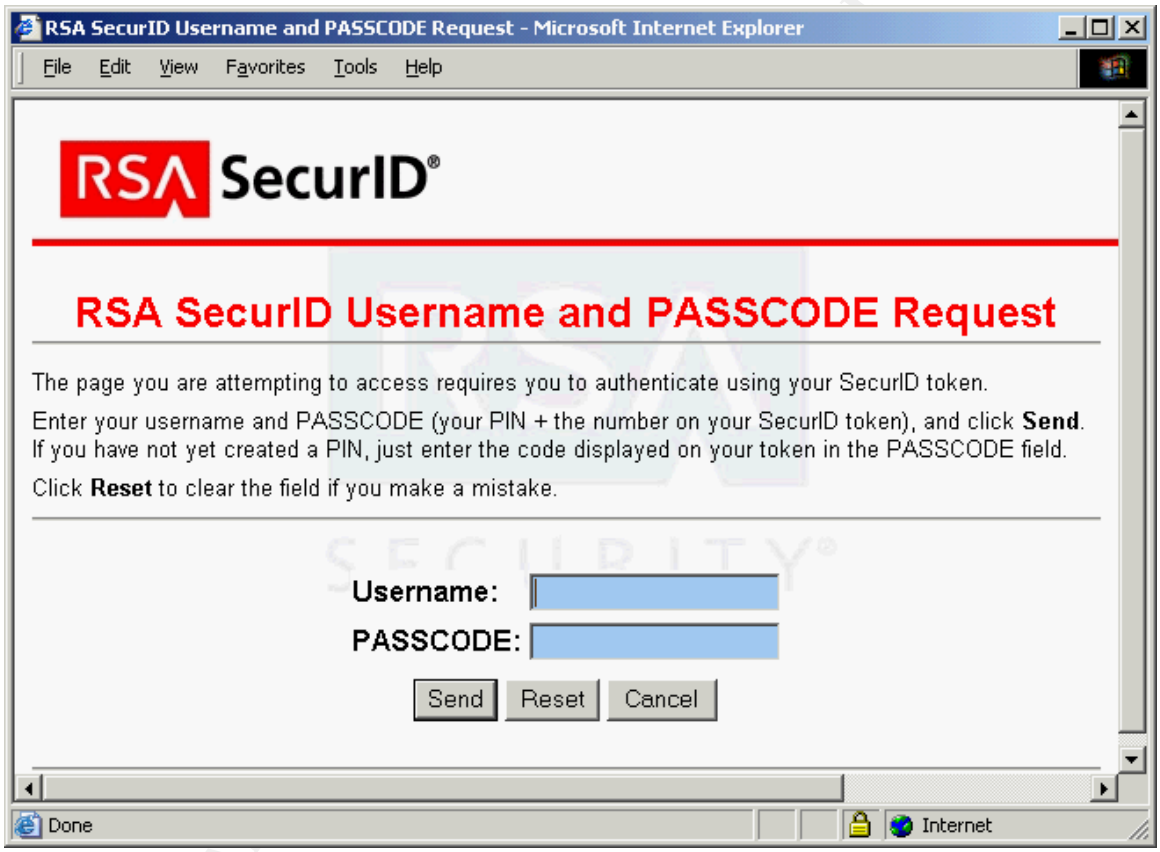

Figure 1. IT-ISAC Login.

Priority II, A National Cyberspace Security Threat and Vulnerability Reduction Program, attempts to establish a plan for identifying weakness in the Internet through various government agencies and technology. Despite the name that suggests otherwise, it is not one program or system under one agency. However, one goal of this priority empowers the federal law enforcement agencies to "reduce threats and deter malicious actors through effective

[24] http://www.infoworld.com/article/03/03/04/HNcybersecurity_1.html?security
[25] http://www.iss.net/

programs to identify and punish them."[26] Programs such as the FBI Infragard and Secret Service electronic crimes taskforces are supposed to glean information from their investigations and report them to the Department of Homeland Security, who will then push the data back to the ISACs. The Department is supposed to establish a nationwide vulnerability assessment or assessments for gauging the impact of possible attacks. Such a task will be daunting considering the scope and number of variables involved. No doubt the Department will look to outside contractors for assistance in developing this project.

The strategy does an excellent job of summarizing some of the intrinsic vulnerabilities in the Internet. Internet Protocol (IP), Domain Name System (DNS), Border Gateway Protocol (BGP) are all given mention. Of significance is the pursuit of Internet Protocol version 6 or IPV6. IPV6, or Ipng[27] (IP next generation), is a protocol under development that solves the problem of lack of IP addresses, data transfer limits, and inherent insecurity in IPV4. The strategy directs the Department of Commerce to form a task force to study IPV6 and its impact on industry segments. Japan plans to use IPV6 exclusively by 2005. China and the European Union are also considering the new protocol.

Other technical innovations sought include out-of-band router management. If a router has become a victim of a Denial of Service attack, administrative access for corrective action is usually prevented. In addition, the strategy fosters what it calls trusted Digital Control Systems /Supervisory Control and Data Acquisition systems (DCS/SCDA) to remotely control systems that once were controlled locally and manually. Trusted authentication, especially considering the importance of certain utility power systems, is crucial to the protection of critical physical infrastructure. The Department of Homeland Security is supposed to coordinate with the Department of Energy on this matter.

One of the most glaring problems of the Internet is the abundance of vulnerable systems for which a known patch is available. Worms and viruses are programmed to take advantage of these weaknesses, instantly and automatically infecting other nodes across the globe. The National Infrastructure Advisory Council is tasked with working with vendors to convince them to subscribe to its method of disclosure and remediation. In addition, the U.S. General Services Administration (GSA)[28] is supposed to develop a patch clearinghouse for the federal government. Other government agencies involved include the Federal Communications Commission[29] and its Network and Reliability Interoperability Council[30] and its National Security Telecommunications Advisory Committee.[31] The National Infrastructure Simulation and Analysis Center will be involved with

[26] *National Strategy to Secure Cyberspace*, p. 28
[27] http://www.webopedia.com/TERM/I/IPng.html
[28] http://www.gsa.gov/Portal/home.jsp
[29] http://www.fcc.gov/
[30] http://www.nric.org/
[31] http://www.ncs.gov/

simulation modeling to judge the impact of certain physical and cyber attacks on our infrastructure.

Alongside the Office of Management and Budget in supervising all federal agencies is the Office of Science and Technology Policy (OSTP).[32] The OSTP was created by the National Science and Technology Policy, Organization, and Priorities Act of 1976 (Public Law 94-282). Its key role is as lead agency on science and technology efforts and as an advisor to the President. The OSTP operates as a research and development agency. The strategy gives the OSTP the mandate of researching emerging technology as part of the National Cyberspace Security Threat and Vulnerability Reduction Program.

One of the most important pieces in the security puzzle is education. The third priority, A National Cyberspace Security Awareness and Training Program, is probably one of the most practical and likely to be carried out. The three components of this priority are Awareness, Training, and Certification. The majority of the content and structure of the *Draft National Strategy to Secure Cyberspace*, with the exception of the federal sector, is found in this section, although in a much-dumbed down version. While the draft was probably meant to be a detailed source document that industry sectors (Home Users and Small Businesses; Large Enterprises; Institutions of Higher Education; other Private Sectors; and State and Local Governments) could reference to secure an organization, the final strategy summarizes common threats and recommendations geared toward each sector. It directs the Department of Homeland Security to create an awareness program similar to the StaySafeOnline[33] campaign, and directs the Department of Education to release funds for primary and secondary schools. The Ad Council[34], established during World War II for the purpose of creating propaganda ads in support of the war would have been a good vehicle for disseminating security awareness. Direct advertising would also work.

Training and Certification are especially critical in the Information Technology and Security industry. Software, protocols, and standards change frequently. A major component of the strategy is to foster programs that support the nation's needs. The Department of Homeland security is to work with the National Science Foundation[35], the Office of Personnel Management[36], and the National Security Agency[37] in ways to bolster the Cyber Corps Scholarship for Service program that was created by the Cyber Security Research and Development Act (Public Law 107-305)[38]. The strategy recognizes that no one certification can cover all knowledge; however, the need for standards in

[32] http://www.ostp.gov/
[33] http://www.staysafeonline.info/
[34] http://www.adcouncil.org/
[35] http://www.nsf.gov/
[36] http://www.opm.gov/
[37] http://www.nsa.gov/
[38] http://www.house.gov/science/cyber.htm

certification is desired. Again the Department of Homeland Security is to work with certification organizations in a voluntary manner to produce training and certificate programs that both the government and private sectors will accept together.

Priority IV, Securing Governments' Cyberspace, reads like a road map for where the government has been and needs to go as far as its own systems are concerned. Technology vendors should be pleased with the statement that "federal agencies should become early adapters of new, more secure systems and protocols where appropriate."[39] The federal government is to lead by example when it comes to security. The path ahead will be a difficult one. According to the strategy, the Office of Management and Budget's first report to Congress in February 2002 stated that there existed the following government-wide security problems:

(1) Lack of senior management attention;
(2) Lack of performance measurement;
(3) Poor security education awareness;
(4) Failure to fully fund and integrate security into capital planning and investment control;
(5) Failure to ensure that contractor services are adequately secure; and
(6) Failure to detect, report, and share information on vulnerabilities.[40]

In 2000 Congress passed the Government Information Security Reform Act (Public Law 106-398) or GISRA. This law placed significant security reporting requirements on government agencies. Agencies were issued report cards on their security status and were asked to justify their grades in front of Congressional hearings. Many security experts were worried when GISRA was set to expire in November 2002. GISRA was replaced with the E-Government Act of 2002 (Public Law 107-347).[41] This significant IT initiative has its own domain name of www.egov.gov. The first part of Priority IV is simply a mandate to follow existing well-known security best practices. The second part lists additional challenges to government. One hurdle that almost all IT systems must jump is how to properly authenticate and authorize users. The strategy references the E-Authentication project[42], part of E-gov, as a way for all departments to use the same authentication system to increase security. The sheer size of the federal government and complex nature of multitudes of agencies makes this initiative unlikely to succeed to completion. However while systems are replaced top-down, with the Office of Management and Budget in control, partial ongoing progress is very likely.

[39] *National Strategy to Secure Cyberspace*, p. 43
[40] *National Strategy to Secure Cyberspace*, p. 44
[41] http://csrc.nist.gov/policies/HR2458-final.pdf
[42] http://www.whitehouse.gov/omb/egov/ea/eauthentication.htm

Securing Wireless got its mention in the strategy, but only a token two paragraphs. Readers are directed to the National Institute of Standards and Technology for information on securing government WLANs. The National Information Assurance Partnership[43] created by the Computer Security Act of 1987 partners the NSA with NIST. NIST did not transfer to the Information Analysis and Infrastructure Protection Directorate of the Department of Homeland Security and its role seems to overlap with that of the Office of Science and Technology Policy, at least on paper. Other specific recommendations include improving government outsourcing and procurement. Lessons learned from the Defense Department policy changes in July 2002 will help determine any new policies set in the future. Lastly, the concept that companies performing security audits be independent (e.g., having no conflicts of interest) will be pursued along with requirements for minimal certifiable security skills.

Priority V, National Security and International Cyberspace Security Cooperation segments non-cyber security responses to cyber attacks and International efforts to respond to cyber attacks. The title of this section reveals that there is still a mental divide between old ideas of what national security has been and what it should be. From this administration, unless there is a "Cyberspace" moniker, it has nothing to do with IT. It is a shame, since the nation has yet to understand what an impact a nationwide Internet outage would have on the economy and as a result the negative impact it would have on our long-term ability to fight terrorism and to enjoy our economic and social freedoms in general.

Nonetheless, the strategy establishes key goals such as strengthening cyberspace counter-intelligence efforts, improving ways of identifying real sources of attacks, and responding to attacks wherever they may occur. Here is a stern warning to the perpetrators of such attacks: "…the U.S. response need not be limited to criminal prosecution. The United States reserves the right to respond in an appropriate manner."[44]

A web surfer in Maine enters http://www.google.com into his browser. His destination may be established through a number of different "hops" that may not even reside in the United States. The global nature of the Internet Protocol, the same design that was intended to provide resiliency in the case of a nuclear attack, makes it possible for an attacker on the other side of the earth to anonymously probe and attack a network. There are no boundaries in cyberspace. Even some of the companies that provide the Internet backbone have no allegiance to any one country. The strategy sets forth to work with other nations and international organizations. The Department of State[45] is the lead

[43] http://www.niap.nist.gov
[44] *National Strategy to Secure Cyberspace*, p. 50
[45] http://www.state.gov/

agency on this effort. Some of these groups include the Organization of Economic Cooperation and Development (OECD), G-8, the Asia Pacific Economic Cooperation forum (APEC) and the Organization of American States (OAS). Specifically ,the US will urge other nations to subscribe to the Council of Europe Convention on Cybercrime, which requires them to make computer cracking a serious offense, and to join the high-tech crime contact network started by the G-8. Substantial progress has been made on this item recently. The United States and France met March 24-26, 2003 to discuss critical infrastructure items during a conference coined the Lyon Group.[46] Tom Ridge, Director of the Department of Homeland Security, shared a press briefing with the British Home Secretary David Blunkett on April 1, 2003 on ways to share common experiences in protecting cyber infrastructure, such as best practices and joint training exercises.[47]

The *National Strategy to Secure Cyberspace* ends with a summary and appendix. Throughout the document specific actions are listed in italics. They are actually useful if one wants to get to the core of what the government plans to accomplish without reading all the extraneous support text. The appendix contains all the action items.

The strategy is not without its critics. "[It's] about as helpful as duct taping servers and wrapping them in plastic sheeting."[48] "In short, a pipe dream … weak willed."[49] "Nothing much in it to brag about."[50] Is the national strategy relevant at all? Will it fulfill its guiding principles of increasing the sharing of information and protecting privacy? Will its basis in non-regulatory enforcement work? The President's policy paper has only been in effect for less than two months. This practical should provide a starting point for future insight into these questions.

---

46 http://www.g8.fr/evian/english/navigation/news/g8_conference_on_the_protection_of_critical_infrastructures.html#topofthepage

47 http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0124.xml

48 Petersen, http://www.eweek.com/article2/0,3959,903205,00.asp.

49 Jerico, http://www.attrition.org/security/rant/z/clarke.html.

50 Desmond, http://itmanagement.earthweb.com/columns/secugud/article.php/2013941.

References

Bush, George W. The National Strategy to Secure Cyberspace. Cover Letter, 2003.

Bush, George W. Executive Order 13231, Section 5; Board Responsibilities, 2001.

National Security Council Web Page. 27 March 2003. URL: http://www.whitehouse.gov/nsc/ (2 April 2003)

National Security Council. The National Security Strategy of the United States of America. September 2002: 31.

President's Critical Infrastructure Protection Board. "Roles and Responsibilities in Securing Cyberspace." The National Strategy to Secure Cyberspace. February 2003: 9.

President's Critical Infrastructure Protection Board. The National Strategy to Secure Cyberspace. February 2003: 17.

President's Critical Infrastructure Protection Board. "Critical Infrastructure Lead Agencies." The National Strategy to Secure Cyberspace. February 2003: 16.

Financial Services Information Sharing And Analysis Center. "The Financial Services ISAC FAQs." URL: http://www.fsisac.com/faq.cfm (2 April, 2003)

President's Critical Infrastructure Protection Board. The National Strategy to Secure Cyberspace. Febrary 2003: 28.

President's Critical Infrastructure Protection Board. The National Strategy to Secure Cyberspace. Febrary 2003: 43.

President's Critical Infrastructure Protection Board. The National Strategy to Secure Cyberspace. Febrary 2003: 44.

President's Critical Infrastructure Protection Board. The National Strategy to Secure Cyberspace. Febrary 2003: 50.

Petersen, Scot. "Cyber Plan Falls Short." 24 February, 2003. URL: http://www.eweek.com/article2/0,3959,903205,00.asp (3 April, 2003)

Jerico. "Richard Clarke: American Grandstand." 4 March, 2003. URL: http://www.attrition.org/security/rant/z/clarke.html (3 April, 2003)

Desmond, Paul. “Fed Cyberspace Security Strategy -- Nothing Much for Everyone.” 3 March, 2003. URL: http://itmanagement.earthweb.com/columns/secugud/article.php/2013941 (3 April, 2003)

Last Updated: April 6th, 2012

Upcoming Training

Mentor Session SEC401 - EMEA - Cairo	**Cairo, Egypt**	**Apr 07, 2012 - Apr 08, 2012**	**Mentor**
Community SANS New York Spring 2012	**New York, NY**	**Apr 09, 2012 - Apr 13, 2012**	**Community SANS**
Mentor Session - AW - SEC401	**San Jose, CA**	**Apr 10, 2012 - Jun 19, 2012**	**Mentor**
SANS Northern Virginia 2012	**Reston, VA**	**Apr 15, 2012 - Apr 20, 2012**	**Live Event**
Community SANS Waterloo	**Waterloo, ON**	**Apr 16, 2012 - Apr 21, 2012**	**Community SANS**
Mentor Session SEC401 - EMEA - Lausanne	**Lausanne, Switzerland**	**Apr 17, 2012 - Jun 19, 2012**	**Mentor**
Mentor Session - SEC 401 - Security boot camp essentials	**Albany, NY**	**Apr 24, 2012 - Jun 26, 2012**	**Mentor**
Community SANS Rockville Spring 2012	**Rockville, MD**	**Apr 30, 2012 - May 04, 2012**	**Community SANS**
SANS Secure Europe 2012	**Amsterdam, Netherlands**	**May 07, 2012 - May 19, 2012**	**Live Event**
Mentor Session - TCP - SEC401	**Sacramento, CA**	**May 09, 2012 - May 16, 2012**	**Mentor**
SANS Security West 2012	**San Diego, CA**	**May 10, 2012 - May 18, 2012**	**Live Event**
Security West 2012 - SEC401 SANS Security Essentials Bootcamp Style - Dr. Eric Cole	**201205 - SEC401, CA**	**May 12, 2012 - May 17, 2012**	**vLive**
Community SANS Portland	**Portland, OR**	**May 14, 2012 - May 19, 2012**	**Community SANS**
SANS Toronto 2012	**Toronto, ON**	**May 14, 2012 - May 19, 2012**	**Live Event**
SANS Brisbane 2012	**Brisbane, Australia**	**May 21, 2012 - May 26, 2012**	**Live Event**
Community SANS Philadelphia 2012	**Philadelphia, PA**	**May 21, 2012 - May 26, 2012**	**Community SANS**
SANS Secure Indonesia 2012	**Jakarta, Indonesia**	**May 28, 2012 - Jun 02, 2012**	**Live Event**
Community SANS Victoria	**Victoria, BC**	**May 28, 2012 - Jun 02, 2012**	**Community SANS**
Mentor Session - SEC 401 Security Boot Camp Essentials	**Lima, Peru**	**Jun 02, 2012 - Jun 23, 2012**	**Mentor**
SANS Rocky Mountain 2012	**Denver, CO**	**Jun 04, 2012 - Jun 09, 2012**	**Live Event**
Community SANS Paris SEC401 @ Lexsi	**Paris, France**	**Jun 06, 2012 - Jun 13, 2012**	**Community SANS**
SANS Geneva Security Essentials at HEG 2012	**Geneva, Switzerland**	**Jun 11, 2012 - Jun 16, 2012**	**Community SANS**
SANS Malaysia 2012	**Cyberjaya, Malaysia**	**Jun 18, 2012 - Jun 23, 2012**	**Live Event**
SANS Canberra 2012	**Canberra, Australia**	**Jul 02, 2012 - Jul 10, 2012**	**Live Event**
SANSFIRE 2012	**Washington, DC**	**Jul 06, 2012 - Jul 15, 2012**	**Live Event**
Community SANS Anaheim 2012	**Anaheim, CA**	**Jul 09, 2012 - Jul 14, 2012**	**Community SANS**
SANSFIRE 2012 - SEC401 - SANS Security Essentials Bootcamp Style - Dr. Eric Cole	**201207 - SEC401, DC**	**Jul 09, 2012 - Jul 14, 2012**	**vLive**
Community SANS Albuquerque	**Albuquerque, NM**	**Jul 09, 2012 - Jul 14, 2012**	**Community SANS**
Community SANS Las Vegas 2012	**Las Vegas, NV**	**Jul 16, 2012 - Jul 21, 2012**	**Community SANS**
SANS Thailand 2012	**Bangkok, Thailand**	**Jul 23, 2012 - Aug 04, 2012**	**Live Event**
SANS San Francisco 2012	**San Francisco, CA**	**Jul 30, 2012 - Aug 06, 2012**	**Live Event**