CI copy #013

THE WHITE HOUSE

WASHINGTON

January 9, 2008

MEMORANDUM FOR RECIPIENTS OF NSPD-54/HSPD-23

SUBJECT: Distribution of NSPD-54/HSPD-23

Attached is your department's or agency's copy of National Security Presidential Directive (NSPD)-54/Homeland Security Presidential Directive (HSPD)-23. Regardless of whether the text is classified or unclassified, this Presidential document should be carefully safeguarded.

Since NSPDs/HSPDs communicate new Presidential policy on sensitive policy and national security topics, copies should be redistributed within your department or agency only on a need to know basis. Broader dissemination of policy decisions, as necessary, should take place by providing a summary of the NSPD/HSPD to appropriate staff or by including relevant portions in department or agency directives or policy guidance.

NSPDs/HSPDs should not be redistributed beyond your department or agency or overseas within your department or agency without the advance approval of the NSC and HSC staffs. Likewise, all public requests for copies of or access to NSPDs/HSPDs, or Presidential Directives of prior administrations, should be referred to the NSC and HSC. All such requests for redistribution should be faxed to HSC's Executive Secretary at 202-456-5158 and NSC's Senior Director for Records and Access Management at 202-456-9200.

David V. Trulio
Special Assistant to the President
and Executive Secretary
Homeland Security Council

cc: John I. Pray, Jr.
Executive Secretary
National Security Council

~~TOP SECRET~~

THE WHITE HOUSE

WASHINGTON

January 8, 2008

NATIONAL SECURITY PRESIDENTIAL DIRECTIVE/NSPD–54
HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD–23

Subject: Cybersecurity Policy (U)

Purpose

(1) This directive establishes United States policy, strategy, guidelines, and implementation actions to secure cyberspace. It strengthens and augments existing policies for protecting the security and privacy of information entrusted to the Federal Government and clarifies roles and responsibilities of Federal agencies relating to cybersecurity. It requires the Federal Government to integrate many of its technical and organizational capabilities in order to better address sophisticated cybersecurity threats and vulnerabilities. (U)

(2) This directive (a) provides an enduring and comprehensive approach to cybersecurity that anticipates future cyber threats and technologies and involves applying all elements of national power and influence to secure our national interests in cyberspace and (b) directs the collection, analysis, and dissemination of information related to the cyber threat against the United States and describes the missions, functions, operations, and coordination mechanisms of various cyber operational organizations throughout the Federal Government. (U)

(3) This directive furthers the implementation of the *National Strategy for Homeland Security*, Homeland Security Presidential Directive-5 (HSPD-5) (*Management of Domestic Incidents*), Homeland Security Presidential Directive-7 (HSPD-7) (*Critical Infrastructure Identification, Prioritization, and Protection)*, Homeland Security Presidential Directive-8 (HSPD-8) (*National Preparedness*), Executive Order 13434 of May 17, 2007, (*National Security Professional Development*), [redacted] ~~(S//NF)~~

(b)(1)
OGA
NSC

(4) Actions taken pursuant to this directive will improve the Nation's security against the full spectrum of cyber threats and, in particular, the capability of the United States to deter, prevent, detect, characterize, attribute, monitor, interdict, and otherwise protect against unauthorized access to National Security Systems, Federal systems, and private-sector critical infrastructure systems. ~~(S//NF)~~

~~TOP SECRET~~
Reason: 1.4 (c) (d) (e) (g)
Declassify on: 1/05/2043

Background

(5) The electronic information infrastructure of the United States is subject to constant intrusion by adversaries that may include foreign intelligence and military services, organized criminal groups, and terrorists trying to steal sensitive information or damage, degrade, or destroy data, information systems, or the critical infrastructures that depend upon them. Cyber criminals are intent on malicious activity, including the manipulation of stock prices, on-line extortion, and fraud. These activities cost American citizens and businesses tens of billions of dollars each year. Hackers and insiders have penetrated or shut down utilities in countries on at least three continents. Some terrorist groups have established sophisticated on-line presences and may be developing cyber attacks against the United States. ~~(S//NF)~~

(6) The United States must maintain unrestricted access to and use of cyberspace for a broad range of national purposes. The expanding use of the Internet poses both opportunities and challenges. The ability to share information rapidly and efficiently has enabled huge gains in private sector productivity, military capabilities, intelligence analysis, and government effectiveness. Conversely, it has created new vulnerabilities that must be addressed in order to safeguard the gains made from greater information sharing. ~~(S//NF)~~

Definitions

(7) In this directive:

(a) "computer network attack" or "attack" means actions taken through the use of computer networks to disrupt, deny, degrade, manipulate, or destroy computers, computer networks, or information residing in computers and computer networks; ~~(S)~~

(b) "computer network exploitation" or "exploit" means actions that enable operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks; ~~(S)~~

(c) "counterintelligence" means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorist activities; (U)

(d) "cyber incident" means any attempted or successful access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, an application, or an information system, without lawful authority; (U)

(e) "cyber threat investigation" means any actions taken within the United States, consistent with applicable law and Presidential guidance, to determine the identity, location, intent, motivation, capabilities, alliances, funding, or methodologies of one or more cyber threat groups or individuals; (U)

(f) "cybersecurity" means prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation; (U)

(g) "cyberspace" means the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries; (U)

(h) "Federal agencies" means executive agencies as defined in section 105 of title 5, United States Code, and the United States Postal Service, but not the Government Accountability Office; (U)

(i) "Federal systems" means all Federal Government information systems except for (i) National Security Systems of Federal agencies and (ii) Department of Defense information systems; (U)

(j) "information security incident" means a "computer security incident" within Federal Government systems (as described in National Institute of Standards and Technology Special Publication 800-61 "Computer Security Incident Handling Guide") or critical infrastructure systems that is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices; (U)

(k) "information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information; (U)

(l) "intrusion" means unauthorized access to a Federal Government or critical infrastructure network, information system, or application; (U)

(m) "National Security System" means any information system (including any telecommunication system) used or operated by an agency, an agency contractor, or other organization on behalf of an agency, where the function, operation, or use of that system involves (i) intelligence activities, (ii) cryptologic activities related to national security,

(iii) command and control of military forces, (iv) equipment that is an integral part of a weapon or weapon systems, or (v) critical to the direct fulfillment of military or intelligence missions; or is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. This definition excludes any system that is designed to be used for routine administrative and business applications such as payroll, finance, or logistics and personnel management applications; (U)

(n) [redacted] ~~(S//NF)~~

(o) "secure" means to defend and protect both military and civilian Government-owned networks; (U)

(b)(1)
OGA
NSC

(p) "State" and "local government" when used in a geographical sense have the meanings ascribed to them in section 2 of the Homeland Security Act of 2002 (section 101 of title 6, United States Code); and (U)

(q) "US-CERT" means the United States Computer Emergency Readiness Team in the National Cyber Security Division of the Department of Homeland Security (DHS). (U)

Policy

(8) Federal agencies shall, consistent with this directive, increase efforts to coordinate and enhance the security of their classified and unclassified networks; increase protection of the data on these networks; and improve their capability to deter, detect, prevent, protect against, and respond to threats against information systems and data. (U)

(9) Federal agencies shall, as required by law, protect the confidentiality, integrity, and availability of information stored, processed, and transmitted on their information systems, and shall ensure the authentication of access to such systems as required. Federal agencies shall take appropriate measures to reduce the risk to these systems and adequately deter, reduce, and limit the loss of information or the operational degradation of information systems that are critical to the national security, national economic security, or public health or safety. (U)

(10) The Federal Government shall increase efforts with critical infrastructure sectors to enhance the security of their information networks. (U)

Policy Coordination

(11) Consistent with National Security Policy Directive-1 (NSPD-1) (*Organization of the National Security Council System*) and Homeland Security Presidential Directive-1 (HSPD-1) (*Organization and Operation of the Homeland Security Council*), the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism shall be responsible to the President for interagency policy coordination on all aspects of cybersecurity. ~~(S)~~

(12) The CSC PCC shall ensure ongoing coordination of the U.S. Government policies, strategies, and initiatives related to cybersecurity; shall monitor actions to implement this directive; and shall keep informed the Assistants to the President referenced in paragraph 11 of this directive. (U)

(13) The National Cyber Response Coordination Group (NCRCG) consists of senior representatives from Federal agencies that have roles and responsibilities related to preventing, investigating, defending against, responding to, mitigating, and assisting in the recovery from cyber incidents and attacks. In the event of a cyber incident, the NCRCG will convene to harmonize operational response efforts and facilitate information sharing consistent with HSPD-5 and the National Response Framework. The NCRCG shall provide advice to the CSC PCC, as appropriate. (U)

Roles and Responsibilities

(14) [redacted] ~~(TS)~~

(15) Unless otherwise directed by the President with respect to particular matters, the Secretary of Homeland Security shall lead the national effort to protect, defend, and reduce vulnerabilities of Federal systems and the Secretary of Defense shall provide support to the Secretary of Homeland Security with respect to such assignment. The Secretary of Homeland Security shall:

(b)(1) OGA NSC

(a) Manage and oversee, through US-CERT, the external access points, including access to the Internet, for all Federal systems;

(b) Provide consolidated intrusion detection, incident analysis, and cyber response capabilities to protect Federal agencies' external access points, including access to the Internet, for all Federal systems;

(c) In coordination with the Director of OMB, set minimum operational standards for Federal Government Network Operations Centers (NOCs) and Security Operations Centers

(SOCs) that enable DHS, through US-CERT, to direct the operation and defense of external access points, including Internet access points, for all Federal systems, which the Secretary will certify and enforce; and

(d) Utilize the National Infrastructure Protection Plan process, in accordance with HSPD-7, to disseminate cyber threat, vulnerability, mitigation, and warning information to improve the security and protection of critical infrastructure networks owned or operated by Federal agencies; State, local, and tribal governments; private industry; academia; and international partners. (U)

(16) The Director of OMB shall:

(a) Direct, to the extent practicable and consistent with national security, the reduction and consolidation of Federal Government external access points, including Internet access points, for all Federal systems; (U)

(b) Annually assess, in coordination with the Secretary of Homeland Security, network security best practices of Federal agencies, recommend changes to policies or architectures that should be applied across the Federal Government, and ensure Federal agencies comply with standards and policies if adopted by the Director; and (U)

(c) Within 180 days after the effective date of this directive, draft an implementation plan, in coordination with the Secretary of Homeland Security, for an agency accountability process to ensure compliance with and the maintenance of mandatory network security practices by Federal agencies. (U)

(17) The Secretary of State, in coordination with the Secretaries of Defense, the Treasury, Commerce, and Homeland Security, the Attorney General, and the DNI, shall work with foreign countries and international organizations on international aspects of cybersecurity. (U)

(18) The Secretary of Commerce shall prescribe, in accordance with applicable law, information security standards and guidelines for Federal systems. (U)

(19) The Secretary of Energy, as authorized in the Atomic Energy Act of 1954 (AEA), as amended, shall, after coordination with the Secretary of Defense and the DNI, prescribe information security standards and guidelines pertaining to the processing of restricted data, as defined in the AEA, in all Federal agencies, as appropriate. (U)

(20) The Secretary of Defense and the DNI shall provide indications and warning information to DHS regarding threats originating or directed from outside the United States. (U)

(21) The DNI analyzes and integrates all intelligence possessed or acquired by the U.S. Government pertaining to cybersecurity. The DNI, as the head of the intelligence community and consistent with section 1018 of the Intelligence Reform and Terrorism Prevention Act (Public Law 108-458), shall implement the policies and initiatives set forth in this directive within and throughout the intelligence community through the DNI's statutory budget, tasking, and intelligence information sharing authorities, in order to ensure appropriate resource allocation and integration of all cybersecurity efforts and initiatives within and throughout the intelligence community. (U)

(22) [redacted] ~~(S//NF)~~

(b)(1)
OGA
NSC

(23) The Secretary of Defense has responsibility for directing the operation and defense of the Department of Defense's information enterprise, including monitoring of malicious activity in its networks. The Secretary of Homeland Security is responsible for protecting Federal systems by supporting information assurance strategies within Federal agencies through the following: compiling and analyzing security incident information across the Federal Government; informing and collaborating with Federal, State, local, tribal agencies, private critical infrastructure sectors, and international partners on threats and vulnerabilities; providing vulnerability mitigation guidance; supporting public and private incident response efforts; and serving as a focal point to protect U.S. cyberspace. (U)

(24) The Secretary of Homeland Security, supported by the Director of US-CERT, and the heads of Sector-Specific Agencies, as defined by and consistent with HSPD-7, shall conduct outreach to the private sector on cybersecurity threat and vulnerability information. (U)

(25) The heads of all Federal agencies, to the extent permitted by law and necessary for the effective implementation of the cybersecurity mission, shall support and collaborate with the Secretary of Homeland Security. Further, all Federal agencies shall align their own network operations and defense capabilities to provide DHS with visibility and insight into the status of their Federal systems and shall respond to DHS direction in areas related to network security, allowing DHS to effectively protect the Federal Government network enterprise. Federal agencies shall continue to execute their responsibilities to protect and defend their networks. (U)

Implementation

(26) The Secretary of Homeland Security shall establish a National Cybersecurity Center ("Center"), headed by a Director, to coordinate and integrate information to secure U.S. cyber networks and systems. To ensure a comprehensive approach to cybersecurity and anticipate future threats, other cyber activities shall inform, enable, and enhance cybersecurity activities as appropriate, and in accordance with the implementation plan described in paragraph 28 of this directive. ~~(S)~~

(27) The Secretaries of Defense and Homeland Security, the Attorney General, and the DNI shall collocate at the Center certain representatives from their respective cybersecurity organizations. Other Federal Government cyber organizations [redacted] shall be collocated or virtually connected as appropriate. ~~(TS//NF)~~

(28) Not later than 90 days from the date of this directive, the Secretary of Homeland Security, in coordination with the Secretary of Defense, the Attorney General, the Director of OMB, and the DNI, shall, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, submit to me for approval an implementation plan that includes details on how authorities will be applied, a concept of operations, and the allocation of required resources for the Center. (U)

(29) The Director of the Center shall:

(a) Be appointed by the Secretary of Homeland Security with the concurrence of the Secretary of Defense, after consultation with the Attorney General and the DNI, and is supervised by the Secretary of Homeland Security; (U)

(b)(1) OGA NSC

(b) Have coordination authority over the directors of the cybersecurity organizations participating in the Center, which means the Director has the authority to require consultation between the offices, departments, or agencies collocated in or virtually connected to the Center; however, this authority does not allow the Director to compel agreement or to exercise command; rather, it creates a consultative structure; (U)

(c) Support the Secretaries of Defense and Homeland Security, the Attorney General, and the DNI in executing their respective cyber missions, including [redacted] and investigation and prosecution of cyber crime; ~~(TS//NF)~~

(d) Ensure that Federal agencies have access to and receive information and intelligence needed to execute their respective cybersecurity missions, consistent with applicable law

and the need to protect national security; (U)

(e) Advise within the executive branch on the extent to which the cyber program recommendations and budget proposals of agencies conform to cybersecurity priorities; (U)

(f) When appropriate, recommend and facilitate the adoption of common doctrine, planning, and procedures across all cyber mission areas; and (U)

(g) Not direct or impede the execution of law enforcement, intelligence, counterintelligence, counterterrorism, [redacted] ~~(S//NF)~~

(b)(1) OGA NSC

(30) Each Federal agency operating or exercising control of a National Security System shall share information about information security incidents, threats, and vulnerabilities with the US-CERT to the extent consistent with standards and guidelines for National Security Systems and the need to protect sources and methods. (U)

(31) The National Cyber Investigative Joint Task Force (NCIJTF) shall serve as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations, with representation from the Central Intelligence Agency (CIA), National Security Agency (NSA), the United States Secret Service (USSS), and other agencies, as appropriate. Under the authority of the Attorney General, the Director of the Federal Bureau of Investigation (FBI) shall be responsible for the operation of the NCIJTF. This authority does not allow the Director of the FBI to direct the operations of other agencies. The Director of the FBI shall ensure that participants share the methodology and, to the extent appropriate, case information related to criminal cyber intrusion investigations among law enforcement organizations represented in the NCIJTF in accordance with paragraphs 32 – 33. (U)

(32) The Attorney General shall, by March 1, 2008, develop and publish an initial version of the Attorney General Guidelines for the NCIJTF, in coordination with the heads of other executive departments and agencies as appropriate. (U)

(33) Within 90 days of the date of this directive, the Attorney General shall submit to the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism an operational plan for the NCIJTF. (U)

Comprehensive National Cybersecurity Initiative

(34) To achieve the goals outlined in this directive, the Federal Government needs an integrated and holistic national approach that builds upon strengths and addresses vulnerabilities in our current cybersecurity practices. This effort shall include the actions directed in paragraphs 35 – 46. (U//~~FOUO~~)

(35) The Director of OMB shall within 90 days of the date of this directive, after consultation with the Secretary of Homeland Security, submit to the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism a detailed plan for the reduction and consolidation by June 30, 2008, of Federal Government external access points, including Internet access points. (U)

(36) The Secretary of Homeland Security shall accelerate deployment of the Einstein program to all Federal systems and shall, after consultation with the Attorney General, enhance the Einstein program to include full-packet content and protocol signature detection. The Secretary of Homeland Security, in consultation with the Director of OMB, shall deploy such a system across the single network enterprise referenced above and consistent with paragraph 16 (a) of this directive no later than December 31, 2008. ~~(S//NF)~~

(37) Within 120 days of the date of this directive, the Secretary of Defense with respect to Department of Defense information systems and the Secretary of Homeland Security with respect to Federal systems, after consultation with the Attorney General,and the Director of OMB, shall develop and submit, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, for my approval an implementation plan to deploy active response sensors across the Federal systems. Such a plan shall also address relevant legal and policy issues of the active response sensor capability. ~~(TS)~~

(38) Within 90 days of the date of this directive, the Director of the Office of Science and Technology Policy (OSTP), after consulting the National Science and Technology Council (NSTC) and the DNI, shall within 90 days of the effective date, develop a detailed plan to coordinate classified and unclassified offensive and defensive cyber research. (U//~~FOUO~~)

(39) Within 45 days of the date of this directive, the DNI, in coordination with the Secretaries of Defense and Homeland Security and the Attorney General, shall submit to the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism a detailed plan, including standard operating and notification procedures, to connect the following cyber centers: NCIJTF; NSA/CSS Threat Operations Center; Joint Task Force-Global Network Operations; Defense Cyber Crime Center; US-CERT; and Intelligence Community Incident Response Center. Within 180 days of this directive, these centers shall be

connected as part of the National Cybersecurity Center. ~~(S//NF)~~

(40) Within 180 days of the date of this directive, the DNI and the Attorney General shall develop a cyber counterintelligence plan, including required resources, that comprehensively reflects the scope and extent of cyber threats. This plan should be consistent with the *National Counterintelligence Strategy of the United States*. (U//~~FOUO~~)

(41) Within 180 days of the date of this directive, the Secretary of Defense and the DNI shall develop a detailed plan to address the security of Federal Government classified networks, including specific recommended measures that will significantly enhance the protection of these networks from the full spectrum of threats. ~~(S//NF)~~

(42) Within 180 days of the date of this directive, the Secretary of Homeland Security, in coordination with the Secretary of Defense, the Director of the Office of Personnel Management, and the Director of the National Science Foundation, shall, within 180 days of the effective date, submit to the Director of the Office of Management and Budget, the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism a report including a strategy and recommendations for prioritizing and redirecting current educational efforts to build a skilled cyber workforce. The report should consider recommendations by such groups as the National Infrastructure Advisory Council, the President's Council of Advisors on Science and Technology, and the National Security Telecommunications Advisory Committee. The report should focus on training the existing cyber workforce in specialized skills and ensuring skilled individuals for future Federal Government employment. (U//~~FOUO~~)

(43) Within 120 days of the effective date of this directive, the Director of the OSTP, after consultation with the NSTC and the DNI, shall develop a plan to expand cyber research and development in high-risk, high-return areas in order to better protect our critical national interests from catastrophic damage and to maintain our technological edge in cyberspace. (U//~~FOUO~~)

(44) Within 270 days of the date of this directive, the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism shall define and develop a comprehensive and coordinated strategy to deter interference and attacks in cyberspace for my approval. ~~(S//NF)~~

(45) Within 180 days of the date of this directive, and consistent with the National Infrastructure Protection Plan and National Security Directive 42 (NSD 42) (*National Policy for the Security of National Security Telecommunication and Information Systems*), the Secretaries of Defense and Homeland Security, in coordination with the Secretaries of the Treasury, Energy, and Commerce, the Attorney General, the DNI, and the Administrator of General Services shall develop a

detailed strategy and implementation plan to better manage and mitigate supply chain vulnerabilities, including specific recommendations to:

(a) Provide to Federal Government and defense acquisition processes personnel access to all source intelligence community vendor threat information;

(b) Reform the Federal Government and defense acquisition processes and policy to enable threat information to be used within acquisition risk-management processes and procurement decisions; and

(c) Identify and broadly implement industry global sourcing risk-management standards and best practices, acquisition lifecycle engineering, and test and evaluation risk mitigation techniques. ~~(S)~~

(46) Within 180 days of the date of this directive, the Secretary of Homeland Security, in consultation with the heads of other Sector-Specific Agencies as outlined in HSPD-7, and consistent with the National Infrastructure Protection Plan, shall submit, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, for my approval a report detailing policy and resource requirements for improving the protection of privately owned U.S.-critical infrastructure networks. The report shall detail how the Federal Government can partner with the private sector to leverage investment in intrusion protection capabilities and technology, increase awareness about the extent and severity of cyber threats facing critical infrastructure, to enhance real-time cyber situational awareness, and encourage specified levels of intrusion protection for critical information technology infrastructure. (U//~~FOUO~~)

(47) Implementing the Comprehensive National Cybersecurity Initiative will require key enablers in the following key areas to ensure success.

(a) The DNI, in coordination with, as appropriate, the Secretaries of State, the Treasury, Defense, Commerce, Energy, and Homeland Security, and the Attorney General, and the Director of OMB, shall:

(i) Monitor and coordinate the implementation of paragraphs 35 through 47 (the "Comprehensive National Cybersecurity Initiative" or "Initiative") of this directive;

(ii) Recommend such actions as the DNI judges necessary to implement the Initiative to:

(A) the President; and

(B) the heads of Federal agencies as appropriate, and the Director of the Office of Management and Budget, for action within their respective authorities; and

(iii) Report not less often than quarterly to the President, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, on implementation of the Initiative, together with such recommendations as the DNI deems appropriate. (U)

(b) The Secretary of Homeland Security and the Attorney General shall ensure adequate support for agents, analysts, and technical infrastructure to neutralize, mitigate, and disrupt illegal computer activity domestically. ~~(S)~~

(c) The Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the DNI, and other heads of Federal agencies as appropriate shall increase predictive, behavioral, information, and trend analyses to better understand and anticipate foreign cyber and technology developments. ~~(S//NF)~~

(d) [redacted] ~~(S//NF)~~

(b)(1)
OGA
NSC

(e) [redacted] ~~(S//NF)~~

(f) [redacted] ~~(TS)~~

(g) The Secretary of Defense and the DNI shall increase Information Assurance to protect National Security Systems against intrusion and attack by implementing defenses to significantly reduce current malicious activity and enable network defenders to focus more effectively on more sophisticated threats. Additionally, by strengthening enterprise-wide cross-domain capabilities and utilizing strong identity protection, the

Federal Government will begin to enable greater information sharing among the key cyber organizations. (U//~~FOUO~~)

(48) Within 180 days of the date of this directive, the Director of OMB, in coordination with the heads of all executive departments and agencies, shall perform a comprehensive risk assessment for the loss, manipulation, or theft of all data currently residing on Federal government unclassified networks. The assessment should assume that adversaries have the capability and intent to either capture the data or disrupt mission applications residing on unclassified networks. The assessment should recommend a prioritized description of which data and applications should be migrated to more secure networks. (~~S//NF~~)

(49) Within 120 days of the date of this directive, the Secretaries of State, Defense, and Homeland Security, the Attorney General, and the DNI shall submit to the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism a joint plan for the coordination and application of offensive capabilities to defend U.S. information systems. (U//~~FOUO~~)

(50) Within 120 days of the date of this directive, the Attorney General and the Secretary of Homeland Security, after coordination with the Secretary of Defense and the DNI, shall submit to the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism a plan for the coordination and application of law enforcement capabilities to better support investigations of cyber incidents in United States networks. (U//~~FOUO~~)

Budget

(51) For all future budgets, the heads of all executive departments and agencies shall submit to the Director of OMB, concurrent with their budget submissions, an integrated budget plan to implement the cybersecurity actions described in this directive, consistent with such instructions as the Director of OMB may provide. (U)

General

(52) To the extent of any inconsistencies between this directive and the *National Strategy to Secure Cyberspace* (2003), this directive shall govern. (U)

(53) This directive:

(a) Shall be implemented consistent with applicable law and the authorities of executive departments and agencies, or heads of such departments and agencies, vested by law

(including for the protection of intelligence sources and methods), and subject to the availability of appropriations;

(b) Shall not be construed to impair or otherwise affect the functions of the Director of OMB relating to budget, administrative, and legislative proposals;

(c) Shall not be construed to alter, amend, or revoke any other NSPD or HSPD currently in effect;

(d) Shall not be construed to apply to special activities as defined in section 3.4(h) of Executive Order 12333 of December 4, 1982;

(e) Shall be implemented in a manner to ensure that the privacy rights and other legal rights of Americans are recognized; and

(f) Is intended only to improve the internal management of the executive branch of the Federal Government, and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person. (U)