(U) Appendix D: Evaluation of the Comprehensive National Cybersecurity Initiative

(U) Presidential Directive NSPD-54/HSPD-23, *Cybersecurity Policy*, established "United States policy, strategy, guidelines, and implementation actions to secure cyberspace." It includes a Comprehensive National Cybersecurity Initiative (CNCI), created to strengthen policies for protecting U.S. Government information and systems, clarify roles and responsibilities of Federal agencies related to cybersecurity, and explore how the Federal government might enhance its relationship with the private sector in order to better protect our critical infrastructures. The resourcing and implementation of the CNCI has been undertaken by the Federal government with a sense of urgency that reflects the nature and severity of the threat. The major "initiatives" within the CNCI are:

- Manage the Federal Enterprise Network as a single network enterprise, with Trusted Internet Connections that collapse the number of portals between government networks and the Internet;
- Deploy consistent intrusion detection capabilities across the Federal enterprise;
- Pursue deployment of intrusion prevention systems across the Federal enterprise;
- Catalogue, coordinate and redirect as appropriate cyber research and development efforts;
- Connect current cyber centers to enhance cyber situation awareness;
- Develop a government-wide cyber counterintelligence plan;
- Increase the security of classified networks;
- Expand cyber education;
- Define and develop enduring "leap-ahead" technology, strategies, and programs;
- Define and develop enduring deterrence strategies and programs;
- Develop a multi-pronged approach for global supply chain risk management; and
- Define the Federal role for extending cybersecurity into critical infrastructure domains by working with the private sector.

(U) These major portions of the CNCI required strengthening key strategic foundational capabilities within the Federal government, hence the CNCI includes several strategic "enablers" that augment ongoing cyber-related activities at specific departments and agencies:

- Ensuring adequate support to neutralize, mitigate, and disrupt domestic illegal computer activity;
- Increasing information assurance programs and activities;
- Increasing predictive, behavioral, information and trend analysis of foreign intrusion activities and computer network operational threats;
- Expanding and enhancing U.S. offensive capabilities in support of network defense;
- Increasing investment in U.S. Government cryptanalysis;
- Developing, deploying, and managing an intrusion response capability; and
- Monitoring and coordinating implementation of the CNCI.

(U) Significant CNCI accomplishments to date include rapid progress on many of the initiatives and their strategic enablers; extensive engagement with the Congress; the development of a consolidated view of the disparate budget resources committed to cyber programs funded under national intelligence, military, information assurance, law enforcement, and civilian agency program budgets; and the initiation of key out-of-cycle resource and acquisition activities that would have been difficult within normal legislative appropriations schedules. As a consolidated portfolio scarcely more than one year in existence, the results achieved have been overwhelmingly positive, and although challenges remain, the objectives are clear and in keeping with the larger strategy. The Federal government should continue to go forward with CNCI implementation.

(U) NSPD-54/HSPD-23 assigned responsibility for monitoring, coordinating, and reporting on implementation of the CNCI to the Director of National Intelligence (DNI), despite the fact that much of the CNCI portfolio falls outside of the Intelligence Community. The DNI has done a commendable and effective job using a Joint Interagency Cyber Task Force (JIACTF) created to carry out these responsibilities. The JIACTF uses a portfolio approach—complete with detailed performance measures and target achievement goals—for tracking the status of the 19 separate initiatives and enablers. Under this approach, the JIACTF serves as the central "steward" for oversight and monitoring, but unlike a traditional joint program management office, individual departments and agencies maintain responsibility for the development of business requirements, program management, and budgeting for each specific initiative and activity.

(U) As anticipated by individual CNCI component implementation plans, much work remains to achieve the objectives of the CNCI program and of NSPD-54/HSPD-23. Progress has been uneven, and subsequent oversight must put greater emphasis on scalability and sustainability. While the "steward" model for monitoring and coordinating CNCI activities has been effective as a start-up approach for a complex, multi-agency portfolio, stronger central coordination and oversight will be required to ensure that the individual components are commensurately resourced and mesh effectively to attain the required joint operating capabilities. Only the White House has sufficiently broad authority to provide the required central leadership. JIACTF-like staff support would be necessary to sustain and strengthen the interagency coordination that has been a hallmark of the CNCI successes. Anticipated outcomes

would include more effective collaboration and development of joint standard operating procedures where needed; more fully integrated program acquisition and management; and accelerated opportunities for technology training and re-use.

(U) The CNCI and associated activities identified by NSPD-54/HSPD-23 must evolve to become key base elements of the broader, updated national cyberspace strategy. Successful programs within NSPD-54/HSPD-23 should proceed apace; other programs are keys to the overall success of the strategy but have not fully matured or achieved their anticipated results. Where necessary, "Go Forward" recommendations should endorse the objectives of these programs and provide new direction for resolving roadblocks as well as considering innovative alternatives to accomplish the objectives.

(U) Status of CNCI Activities

(U) The JIACTF, in its "monitoring and coordinating" role, has highlighted areas of concern with CNCI implementation and recommended areas for course correction and has highlighted successes within the CNCI that could be expanded as the program advances. The 60-day cyberspace review team, based on inputs from the JIACTF, the Office of Management and Budget (OMB), and the departments and agencies, makes the following observations about the various CNCI components:

(U) Initiative #1. **Manage the Federal Enterprise Network as a single network enterprise, with Trusted Internet Connections (TICs).** Currently, Federal government networks have thousands of Internet access points that have proven to be too difficult to manage and secure. This Initiative, the primary purpose of which was publicly announced in November 2007,[106] aimed to cut the number of portals between government and the Internet to fewer than 100, using the General Services Administration award of the NETWORX contract for telecommunications service and the Federal Desktop Core Configuration (FDCC) to implement secure desktop configurations. *These program goals and timeframes have proven to be overly ambitious: the TIC and NETWORX consolidation initiative is behind schedule and unlikely to achieve its goal of delivering less than 100 connections either in short- or mid-term timeframes.*

(U) Initiative #2. **Deploy an intrusion detection system of sensors across the Federal enterprise.** Intrusion Detection requires software to identify when unauthorized entities have gained access to computer networks. The Department of Homeland Security (DHS) EINSTEIN 1 software package offers "after the fact" analysis of network flow information from participating Federal agencies and provides a high-level perspective from which to observe potential malicious activity in computer network traffic. The updated version, EINSTEIN 2, incorporates network intrusion detection technology capable of alerting the U.S. Computer Emergency Readiness Team (US-CERT) in real time to the presence of malicious or potentially harmful computer network activity in federal executive agencies' network traffic based on specific pre-defined signatures derived from known malicious activity. DHS reviewed the legal and privacy implications of this system and published a Privacy Impact Assessment for EINSTEIN 2 on its website,[107] thereby providing greater transparency for this part of the CNCI than for most of the other program elements. *Unfortunately, EINSTEIN 2 was envisioned for deployment at the Trusted Internet Connections established by Initiative #1—and hence this Initiative's deployment schedule has slipped because of the slippage in the TIC and NETWORX consolidation.*

[106] (U) http://www.whitehouse.gov/omb/memoranda/fy2008/m08-05.pdf
[107] (U) http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf

(S//REL TO FVEY) Initiative #3. **Pursue deployment of intrusion prevention systems across the Federal enterprise.** Intrusion prevention requires a capability to not only identify intrusions in progress, but to block the attacker from successfully entering the network. Work is under way on developing EINSTEIN 3, a sensor-based system that will automatically block or otherwise mitigate the impact of attempted cyber intrusions. In practice, intrusion prevention is a capability required and routinely deployed by private industry, typically through managed security services offered by Internet Service Providers and Data Exchange Internet Exchange Points, and for home users through commercially available firewall and antivirus programs. The Initiative #3 plan offers advantages unavailable commercially, in particular NSA cryptanalysis and decryption services to address threats masked by encryption. The linkage of EINSTEIN 3 to the NSA Signals Intelligence system, similar to the system already being deployed to defend Department of Defense networks, raises civil liberties and privacy concerns that have significantly complicated EINSTEIN 3 development. *The need for sophisticated intrusion prevention capabilities for government networks is beyond question. There also is a need for greater transparency and public dialogue on the means by which this will be accomplished, taking into account civil liberties and privacy concerns while remaining mindful of the need to protect from release any information that would allow adversaries to subvert U.S. defenses. Given the significant challenges facing this implementation as well as those of Initiatives #1 and #2, EINSTEIN 3 implementation should proceed with a) enhanced transparency and dialogue to address civil liberties and privacy concerns, and b) concurrent assessment of additional implementation concepts that could reduce risks to program implementation while meeting the goals and objectives of Initiative #3.*

(U) Initiative #4: **Coordinate and redirect research and development efforts.** No single individual or organization is aware of all of the cyber-related R&D activities being funded by the Federal government. This Initiative remains critical to determining whether there is redundancy, figuring out research gaps, and ensuring the taxpayers are getting full value for their money as we shape our strategic investments. *Our review determined that a successful process has been created, and the government is beginning to identify shortfalls needing additional investment and those where overlap exists.*

(U) Initiative #5: **Connect current cyber centers to enhance situation awareness.** There is a pressing need to ensure that government information security offices and cyber operations centers share data as legally appropriate regarding malicious activities against federal systems in order to have a better understanding of the entire threat to government systems. This effort focuses on key aspects necessary to enable practical mission bridging across the elements of U.S. cyber activities: network connectivity, common information standards, and shared standard operating procedures. *The review determined that full connectivity at all levels of data classification does not yet exist between the centers, and the continued use of disparate toolsets complicates the development of common situation awareness. The success of this Initiative requires reconsideration of its governance structure and its resourcing requirements.*

(U) Initiative #6: **Develop a government-wide cyber counterintelligence (CI) plan,** encompassing development of a plan across agencies to identify, analyze, share information, and respond as appropriate to foreign-sponsored cyber intelligence threats to the United States. This government-wide Cyber CI Program plan is aligned with the *National Counterintelligence Strategy of the United States of America*—which predates the creation of the CNCI—and supports the other programmatic elements of the CNCI. *The plan is in place and execution is under way, although out-year funding remains a concern*.

(U) Initiative #7: **Increase the security of our classified networks.** These are the networks that house the Federal government's classified and most sensitive information. *A detailed implementation plan has been approved for some Federal government components, although issues surrounding the authorities needed to enforce the plan remain unresolved, as do funding concerns associated with government-wide implementation.*

(U) Initiative #8: **Expand cyber education.** There are too few cybersecurity experts within the Federal government or private sector to adequately implement the CNCI, nor is there an adequately established Federal cybersecurity career field to build upon. Cyber training and personnel development programs, while good, are limited in focus and lack unity of effort. In order effectively to address the scope of the cyber threat, we must develop a technologically-skilled and cyber-savvy workforce and ensure an adequate pipeline for the future. *Our review concluded that the current effort is behind schedule, lacks focus, and requires additional senior level policy guidance.*

(U) Initiative #9: **Define and develop enduring "leap-ahead" technology, strategies, and programs.** One goal of the CNCI is to develop technologies that provide increases in cyber security by orders of magnitude above our current systems and which are deployable 5 to 10 years hence. The Federal government has begun to outline Grand Challenges for the research community to help solve these hard problems, which require "out of the box" thinking. In dealing with the private sector, the government is identifying and communicating common needs that should drive mutual investment in key research areas. In this regard, the government has publicly issued three Requests for Input.[108] *An approved plan is in place and is proceeding well, although some elements are behind schedule in implementation.*

(U) Initiative #10: **Define and develop enduring deterrence strategies and programs.** Senior U.S. policymakers must think through the long-range strategic options available to the United States in a world that depends on assuring the use of cyberspace. To date, the U.S. Government has been implementing traditional approaches to the cybersecurity problem, and these measures have not achieved the level of security needed. *This Initiative is proceeding methodically to build an approach to cyber defense strategy that deters interference and attack in cyberspace using such tools as warning and communication of "red lines", roles for private sector and international partners, and appropriate response by both state and non-state actors. Outreach to a number of key constituencies that can contribute to the development of this strategy has been successful. Out-year funding remains a concern and implementation of the previously approved strategy is lagging.*

(U) Initiative #11: **Develop a multi-pronged approach for global supply chain risk management**. Today's information technology marketplace often provides insufficient software assurance, hardware assurance, or data integrity assurance. Risks stemming both from the domestic and globalized supply chain must be managed in a strategic and comprehensive way over the entire lifecycle of products, systems and services. *Managing this risk requires greater awareness of the threats, vulnerabilities, and consequences associated with acquisition decisions; development and employment of tools and resources to mitigate risk technically and operationally across the lifecycle of products (from design*

[108] (U) As stated on the website of the Networking and Information Technology Research and Development (NITRD) Program, "[O]ver 160 responses were submitted to the first RFI issued by the NITRD SSG (October 14, 2008), indicating a strong desire by the technical community to participate. RFI-2 (issued on December 30, 2008) expanded the opportunity for participation by permitting submitters to designate parts of submissions as proprietary. RFI-3 presents prospective cyber security categories derived from responses to RFI- 1 for further consideration." http://www.nitrd.gov/leapyear/NCLY_RFI-3.pdf

through retirement); and development of new acquisition policies and practices that influence industry to develop and adopt supply chain and risk management standards and best practices. One significant Federal component—the Department of Defense—has issued policy guidance assigning roles and responsibilities and is proceeding to pilot implementation of its approach. This Initiative must continue with increased emphasis on expanding education about supply chain risks and on including more government and private sector communities.

(U) Initiative #12. **Define the Federal role for extending cybersecurity into critical infrastructure domains**. Dialogue about cyber security between the Federal government and the private sector (which owns and operates most of the U.S. critical cyber infrastructure) is essential and has been ongoing for well over a decade. It is widely accepted that the government needs to gain and share with the private sector an operational understanding of how adversaries create and exploit our cyber vulnerabilities, including an assessment of the extent and reach of these adversarial activities and informing the private sector of what is being targeted and, if possible, why. *Progress is being made on multiple fronts, but the government's efforts are not well aligned and, as a result, create an undue burden on private-sector entities that wish to work with the government but cannot commit the resources necessary to participate in multiple forums. As a result, this Initiative should proceed while cataloguing current efforts, determining overlaps and gaps, and communicating in a more streamlined manner with industry.*

(S//REL TO FVEY) Strategic Enablers:

- **Ensure adequate support to neutralize, mitigate, and disrupt domestic illegal computer activity.** *This law enforcement-led activity has made significant operational progress, especially with respect to the establishment and implementation of the FBI's National Cyber Investigative Joint Task Force.*

- **Increase Information Assurance programs and activities:** *This activity is making progress and is poised to serve as a model for wider Federal adoption.*

- **Increase predictive, behavioral, information and trend analysis of foreign intrusion activities and computer network operational threats:** *Foundational work to build the requisite workforce and analytic framework is under way consistent with the strategic plan.*

- **Increase investment in U.S Government cryptanalysis:** *Capabilities are under development.*

- **Develop, deploy, and manage an intrusion response capability:** *Substantial research and development is under way, and capabilities are being field tested within the Department of Defense's .mil environment.*

- **Monitor and coordinate implementation of the CNCI:** *The Joint Interagency Cyber Task Force model of a "steward" coordinating implementation has worked for the CNCI's start-up operations, but is not scalable or sustainable over the entire life-cycle of the program. It should evolve to a stronger central White House leadership effort.*

(U) The following table provides an overview of the status of the CNCI programs along with major recommended actions. The strategic goals of each of the CNCI programs are sound. An evaluation of

"Green" reflects that the strategy is sound and its implementation is proceeding as expected; "Yellow" indicates that progress is lagging and requires attention but that successful implementation of the strategy is still expected; "Orange" indicates that alternative strategies should be considered but work should continue in the meantime; "Red" indicates that implementation is so far off course that an alternative strategy is required.

This table is S//REL TO FVEY

CNCI Initiatives	Recommendation	Evaluation
Initiative 1: *Trusted Internet Connections*	• Review and re-baseline implementation schedule and approach • Subsequent strategy must incorporate all connection types (SATCOM, Wi-Fi, Cable) • Reconcile implementation timeframes with other Federal legislation (stimulus investments, omnibus budget provisions) • Evaluate alternatives for achieving compliance with security objectives	Orange
Initiative 2: *Deploy Passive Sensors Across Federal Systems*	• In light of Initiative 1 delays, continue Einstein 2 while evaluating complementary approaches to achieve Initiative 2 goals • Engage Congress and private sector interests in public dialogue regarding intrusion detection approaches and U.S. Government requirements	Orange
Initiative 3: *Deployment of Intrusion Prevention Systems*	• Engage Congress and private sector interests in public dialogue regarding intrusion prevention approaches and U.S. Government requirements • Work with the Attorney General, OMB, White House, and the Office of the DNI to fulfill legal, civil liberties, and privacy requirements already described in implementation plans • Assess additional implementation concepts that could reduce risks to program implementation while meeting the goals and objectives of Initiative #3	Yellow
Initiative 4: *Coordinate and Redirect Research and Development Efforts*	• Continue as planned	Green

This table is S//REL TO FVEY

CNCI Initiatives	Recommendation	Evaluation
Initiative 5: ***Connect Current Cyber Centers To Enhance Situational Awareness***	• Identify resources to proceed with connectivity or for collocation of centers • Develop integrated program/budget/ governance strategy for ensuring that individual tool capabilities may be acquired and used by all participants • Establish data and product standards and an operational framework for common situation awareness and reporting	Yellow
Initiative 6: ***Develop a Government-Wide Cyber Counter-intelligence Plan***	• Evaluate as objectives are reached • Need to ensure agencies are programming funds for next program build in order to pay for activities	Green
Initiative 7: S*ecure Classified Networks*	• Evaluate as milestones reached • Need to ensure agencies are programming funds for next program build in order to pay for activities	Green
Initiative 8: ***Expand Cyber Education***	• Completely reshape to include a strategy for national-level leadership, comprehensive training programs, and broad-based public dialogue	Red
Initiative 9: ***Define and Develop Enduring Leap-Ahead Technology, Strategies, and Programs***	• Need to accelerate program activities	Yellow
Initiative 10: ***Define and Develop Enduring Deterrence Strategies and Programs***	• Need to implement key recommendations from previously approved strategy	Yellow
Initiative 11: ***Develop Multi-Pronged Approach for Global Supply Chain Risk Management***	• Continue to identify pilot programs • Determine resource requirements for threat evaluation support to all departments and agencies • Evaluate existing legal framework for effecting rapid, threat-based procurement	Yellow
Initiative 12: ***Define the Federal Role for Extending Cybersecurity into Critical Infrastructure***	• Accelerate review of policy, legal, process, and resource barriers • Ensure agencies are programming funds for next program build • Catalogue, distinguish, and align current public/private partnerships	Yellow

This table is S//REL TO FVEY

CNCI Enablers		
Ensure Adequate Support To Neutralize, Mitigate, and Disrupt Domestic Illegal Computer Activity	• Consider how to expand capacity between and among federal, state and local law enforcement entities	Green
Increase DoD Information Assurance	• Evaluate mechanisms for deploying capabilities more quickly • Increase cybersecurity policy training efforts	Green
Strategic Analysis of Intrusion Activities and CNO Threats	• Evaluate how this analytic effort will dovetail with other departments and agencies	Yellow
Increase Investment in U.S Government Cryptanalysis	• Continue long-term investment • Evaluate additional national cybersecurity needs	Green
Develop, Deploy, and Manage an Intrusion Response Capability	• Continue to evaluate solution • Resolve issues associated with adaptability for extending to state, local and private sectors	Yellow
Monitor and coordinate CNCI	• Identify single National Cyber Mission Owner • Reaffirm CNCI roles and responsibilities to maintain momentum	Green