Redactions pursuant to
(b)(1), (b)(3) and (b)(6)
exemptions

Intelligence Science Board

(U//FOUO) Technical Challenges of the National Cyber Initiative

January 24, 2008

ISB
Intelligence Science Board

[redacted]

(U//FOUO) "Technical Challenges of the National Cyber Initiative" – An Assessment by the Intelligence Science Board

(U) Executive Summary

(U//FOUO) The United States no longer controls the fields of information technology (IT) and telecommunications. Irreversible trends in the globalization of IT research, design, manufacturing, and services demand that we adapt our business practices to reflect the realities of the 21st century. The National Cyber Initiative represents an attempt to launch a critically needed transformation in our internal culture and traditional ways of doing business.

(U//FOUO) For the past several years, the Intelligence Science Board (ISB) has advised the Director of National Intelligence (DNI) and the Intelligence Community (IC) at large on issues pertaining to cybersecurity, privacy and security, public-private partnerships for intelligence, and ways to sustain our national abilities in science and technology. We have sought to draw attention to a wide variety of critical vulnerabilities for our nation – including cybersecurity – and have issued repeated calls for a national-level response.

(U//FOUO) The ISB strongly supports the DNI's attempts to establish the National Cyber Initiative, and encourages the nation to continue along the paths laid out. We also applaud the DNI for turning the IC's collective attention to the challenges posed by cyber vulnerabilities, and we encourage the Congress to fully engage with the Administration in helping to fund, guide, and monitor our national efforts. At the same time, the ISB cautions that the need for serious oversight should not impede the first priority: actually launching the overall program. We expect the program to grow and evolve as it matures and gains momentum. Agility in program management and direction will be essential as we learn as a nation how to proceed with this Initiative.

(U//FOUO) No segment of our national society is immune to cyber attack, and no segment of our society can solve this problem alone. The Administration can contribute to a solution by maintaining the prime objective (mission assurance) at the forefront of the national consciousness. Congress can contribute by assessing the complexities of overlapping laws and competing equities and remediating conflicts where appropriate, while keeping the individual program elements intact. The private sector can contribute by supporting the objectives of this Initiative and supplying the labor, tools, and ingenuity necessary to preserve the integrity of our national information. The National Cyber Initiative represents a reasonable first step in a broader effort that should proceed, even as it must be continually refined and improved.

(U//~~FOUO~~) Introduction: A National Crisis Warrants a National Initiative

(~~S~~) Our nation is under attack – not a direct assault on our formidable military and strategic forces, but an ongoing and insidious series of attacks on our automated information systems and networks. Some of these attacks are quite visible (if anyone knows where to look), but some are deliberately stealthy, and therefore may not be detected until well after the fact – if at all. Some attacks are merely nuisances (the digital equivalent of graffiti), but some may have the potential for creating quite serious damage (facilitating espionage, spreading terror and confusion, or disabling our ability to respond militarily in any organized fashion).

(U//~~FOUO~~) For the past several years, the Intelligence Science Board (ISB) has advised the Director of National Intelligence (DNI) and the Intelligence Community (IC) at large on issues pertaining to cybersecurity [1, 2, 3]; privacy and security [4, 5], public-private partnerships for intelligence [6, 7], and ways to sustain our national abilities in science and technology [7, 8, 9]. We have sought to draw attention to a wide variety of critical vulnerabilities for our nation – again including cybersecurity – and have issued repeated calls for a national-level response.

(U//~~FOUO~~) In January 2008 Congress asked the ISB to review the strategy and plans for the National Cyber Initiative [10] and to comment on the technical feasibility and challenges of the current approach. The ISB formed a small task force of four members who, over a period of three weeks, read through the available documentation and interviewed selected government officials regarding the intent behind the plan. This report constitutes the ISB's quick-response technical assessment of the National Cyber Initiative. Given our prior explorations into this broad topic area, our remarks are primarily strategic-level comments about the technical challenges of this endeavor, including potential extensions to the overall Initiative as developed so far.

(~~S~~//[redacted]) The ISB notes that many of the issues and concerns raised in our earlier reports have been taken to heart in shaping the National Cyber Initiative. In particular, the plan provides a forum for national leadership in this complex area. It also includes specific objectives to "raise the bar" of entry for would-be cyber-interlopers into federal cyber systems and to strengthen the security of our classified networks. [redacted]

(U//~~FOUO~~) While a segment of government and private industry has always concerned itself with cybersecurity, both a broader base of stakeholders and more focused examination of the national implications of cyber threat have emerged in recent years. The Federal Government has commissioned several other major studies to address some of our most challenging cyber issues. They include the Defense Science Board (DSB) studies on microchip supply and software assurance [11, 12], the Committee for National Security Systems (CNSS) study on supply chain threats [13], and the United States Telecommunications Infrastructure (USTI) study on telecommunications infrastructure security [14]. The ISB notes that these studies informed and influenced the National Cyber Initiative plan, and we encourage planners to continue to leverage the studies' many actionable recommendations and the cadre of subject matter experts who supported them.

(U//FOUO) The ISB agrees with the overall approach put forward in the Initiative, but wishes to highlight a few key concepts in this report. The ISB understands that cyberspace represents the premiere battlespace for future conflict, and that the thrust of future cyber warfare will not be limited to our military and the Defense Department. In future cyber conflict, *all* our computer systems and digital data (public and private) will be potential targets of attack (possibly simultaneous and possibly strategically coordinated attack). The ISB applauds the DNI's attempts to establish this Initiative and encourages the IC to continue along the paths laid out. We offer the following additional strategic comments to Congress, the President, and the nation about this critical endeavor.

(U//FOUO) We Need a Truly National Approach

(U//FOUO) The ISB notes that while the National Cyber Initiative purports to be a *national* plan, it is, in fact, primarily a *federal* plan aimed at strengthening the cyber defenses of the Federal Government. The ISB agrees that federal defenses do indeed need strengthening and do represent a primary target for adversarial attack. However, no segment of our national society is immune to cyber attack, and no segment of our society can solve this problem alone. The overall problem requires a national solution that involves not only the Federal Government but also state and local governments, the private sector, and the public at large. This Initiative must pursue a successful partnership strategy to engage all of these participants in a mutually beneficial relationship, with the Federal Government playing a leadership role in orchestrating efforts for our common defense.

(S) [redacted]

(b)(1)
(b)(3)

(S//[redacted]) [redacted]

(U//~~FOUO~~) While the ISB strongly encourages the Federal Government to proceed with the National Cyber Initiative, we also encourage the Congress, the President, and others to remember that this Initiative is just the start of a far broader effort. The government must keep cybersecurity at the forefront of national attention and not lapse into the comfortable belief that launching the National Cyber Initiative equates to solving the problem.

(U//~~FOUO~~) Extensive Cooperation and Participation Are Essential

(U//~~FOUO~~) The ISB notes that the plan expressed in the National Cyber Initiative emphasizes Federal Government roles and responsibilities. The issues addressed by this Initiative, however, are fundamental to the continued ability of *any* organization – public or private – to perform its intended mission. We cannot afford to let partisan politics or bureaucratic competition weaken our resolve to address this issue of common concern.

(U//~~FOUO~~) All sectors must devote extensive effort to improving our posture against cyber attack. While the government must assign leadership roles and operational responsibilities to particular individuals and organizations, the overall job is too important to our continued national well-being to entrust to any single organization, branch of government, or segment of our society.

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

(U//~~FOUO~~) The ISB applauds the DNI for turning the IC's collective attention to the challenges of cyber vulnerabilities. We further encourage the Congress to fully engage with the Administration in helping to fund, guide, and monitor our national efforts.

(b)(1)

(U//~~FOUO~~) Mission Assurance Is at Stake

(U//~~FOUO~~) Digital automation and information systems permeate every aspect of modern life, from health care delivery to human social program administration, from communications to commerce, from manufacturing to marketing, from transportation to teleworking, from agriculture to aeronautics and space, from education to entertainment, from legislation to law enforcement, and from diplomacy to defense. The pull of automation is irresistible, and the efficiencies demanded by global competition are irreversible. It would be difficult to think of an enterprise activity whose mission is not profoundly intertwined with information and communications technologies.

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

[redacted]

(b)(1)

(S) The ISB has previously recommended that enterprises in the National Security Community develop contingency plans for continuing mission-critical operations in the event that their data on supporting computer systems and networks are compromised or otherwise rendered unavailable. We note that while some organizations in the public sector already have in place methods for preserving the continuity of mission-critical operations, this advice applies equally well to all enterprises (public and private, large and small) across our society. Broader work, beyond the current scope of the Cyber Initiative, is needed to establish requirements, approaches, and expectations for mission assurance.

(U//FOUO) Complex National Issues Demand a Comprehensive and Complex Response

(S) The National Cyber Initiative comprises some twelve sub-goals or initiatives. Each of these sub-initiatives was crafted to address a particular aspect of the overall national need. Yet critical interrelationships among the sub-initiatives cannot be ignored.

(U//FOUO) To help decision-makers cope with the details of such an enormous undertaking, the overall description of the Initiative has been broken into specific programmatic chunks. Such division between topics, however, may lead to separate assessment of the individual components or even piecemeal funding of components that are either more readily understood or more clearly expressed than the others. Congress can counteract this by assessing the complexities of overlapping laws and competing equities of the overall program and remediating conflicts where appropriate, while keeping the individual program elements intact.

(U//FOUO) The ISB cautions that while serious oversight is required, the first priority must be actually to launch the overall program. We expect the program to grow and evolve as it matures and gains momentum. Agility in program management and direction will be essential as we learn as a nation how to proceed with this Initiative.

(U//FOUO) The Long War of Cyber Conflict Requires a Strategic View

(S) Cyber warfare should be viewed as yet another "long war" in which no "silver bullet" can bring victory. For as long as our society relies on automated information technology (IT) we will be vulnerable to adversaries' attempts to subvert or attack it. Like it or not, this paradigm of cyber conflict applies to all sectors over the long term. But we are not totally defenseless. We do have methods for improving our cybersecurity, as well as a commercial industry that provides cybersecurity information, tools, and products. Both the private and public sectors have developed best practices – practices that must continually be improved and rigorously applied to address a continually evolving threat.

(U//FOUO) A critical issue identified in the National Cyber Initiative is the ongoing need to develop and maintain a competent and knowledgeable cybersecurity workforce. As stated in the Education sub-initiative, a large pool of workers with cybersecurity skills will be essential to staying ahead of the competition in the continual "arms race" of attack-and-defend in cyberspace. This workforce cannot be outsourced to another country. Therefore, as the National Academy of Sciences pointed out [15], the United States must nurture and sustain the next generation of cyber workers.

(C) The ISB notes that the Education sub-initiative is primarily aimed at improving the cybersecurity skill levels of our national workforce. While we agree with this goal, we also suggest that the nation should undertake a broader national educational initiative to make all our citizens and corporations more aware of the extent of the cyber threat and of the need to follow safer computing practices diligently.

(U//FOUO) Effective Implementation Will Demand an Effective Assessment of Trade Spaces

(b)(1)

(S//[redacted]) [redacted]

(S//[redacted]) [redacted]

(S//[redacted]) [redacted]

[redacted]

(S//[redacted]) [redacted]

(U//FOUO) Macro-Level Metrics for Measuring Risk Are Also Needed

(U//FOUO) The ISB is pleased to see that the plan includes some indication of *performance* measures (metrics). While these measures apply largely at the sub-initiative level, they focus initially on measuring *steps taken* as opposed to measuring *progress made*. We would expect that the DNI will develop more robust performance measures during the initial phases of the program.

(C) [redacted]

(S//[redacted]) [redacted]

(U//FOUO) Particularly Challenging Areas Warrant Closer Attention

(U//FOUO) The ISB cautions the government against underestimating the difficulty of achieving the goals of the National Cyber Initiative. We agree with the CIA's characterization of the problem as being on the scale of a "Manhattan Project" – both in the size and complexity of the undertaking and in its technical risk [17]. In fact, the ISB believes that in many respects the cyber problem is the more difficult one, because it pervades all sectors of society and involves more equities. Simply sustaining

(b)(1)

collaboration and cooperation across organizational boundaries – among Federal agencies, between the Federal Government and state or local government entities, between the public and private sectors, and among potentially competing private sector enterprises – will pose enormous challenges.

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

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

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

(S//[redacted]) [redacted]

(S//[redacted]) Beyond the ability to find and identify cyber intrusions, being able to irrefutably *attribute* those intrusions to specific individuals, organizations, or nations will be critical to enforcing any serious policy on deterrence. Simply observing the event will usually not suffice to identify the actor – especially a sophisticated actor. The nation will need to employ and link additional sources of intelligence to connect events, actors, and intent in any compelling way. Doing so rapidly during a live event may require substantial preparation and advanced work.

(U//FOUO) The ISB stresses the importance of sustaining a robust cybersecurity research and development program – a program that is well integrated with ongoing operational efforts to deploy current security technology. The ISB applauds the individual efforts of the Community's cybersecurity research managers and encourages them to extend their efforts to integrate the research community for more effective collaboration.

(U//FOUO) Fostering a National Transformation Requires Broad Cooperation

(U//FOUO) Transforming an enterprise (let alone a nation) is a long and complicated process. The National Cyber Initiative represents an attempt to launch such a transformation – a critically needed transformation in our internal culture and traditional ways of doing business. The global playing field has changed, and the United States no longer controls the fields of IT and telecommunications. Irreversible trends in the globalization of IT research, design, manufacturing, and services demand that we adapt our business practices to reflect the realities of the 21st century.

(S) The ISB is encouraged by the objectives of the Initiative to build bridges between offense and defense, between national security and civil agencies, and between the public and private sectors. We understand that completing such bridges (let alone traversing them) will not be easy and that pressures will grow to slide back to business as usual. The Administration can contribute to meeting the Initiative's goals by keeping the prime objective (mission assurance) at the forefront of the national consciousness. Congress can contribute by assessing the complexities of overlapping laws and competing equities and remediating conflicts where appropriate. The private sector can contribute by supporting the objectives of this Initiative and supplying the labor and tools and ingenuity necessary to preserve the integrity of our national information.

(S) The government must continue to debate how best to tackle the challenges inherent in the Initiative, but there should be no debate on whether to act. Our nation is in peril. The National Cyber Initiative represents a reasonable beginning in a broader effort that should proceed, even as it must be continually refined and improved.

(U) Task Force Participants

(U//~~FOUO~~) Task Force Members

[redacted]

(b)(3)
(b)(6)

(U//~~FOUO~~) Task Force Support

[redacted]

(b)(3)

(U) References

1. (U//~~FOUO~~) Intelligence Science Board Report on *The Impact of Globalization on Foreign Information Operations* [redacted] January 2007.

2. (U//~~FOUO~~) Intelligence Science Board Report on *Rapidly Advancing Globalization and the Emerging Threat of Foreign Information Operations* [redacted], January 2007.

3. (U//~~FOUO~~) Intelligence Science Board Report on *Intelligence Community Cyber Security Research and Development Gaps* [redacted] planned for release February 2008.

4. (U//~~FOUO~~) Intelligence Science Board Letter to *DGC/ODNI on Issues with Privacy, Security, and Technology* [redacted] February 2006.

5. (U//~~FOUO~~) Intelligence Science Board Letter to *DDCI/CM on Issues with Privacy, Security, and Technology* [redacted], December 2004.

6. (U//~~FOUO~~) Intelligence Science Board Executive Forum on *Self-Organizing Information Networks* [U//FOUO], August 2002.

7. (U//~~FOUO~~) Intelligence Science Board Executive Forum on *The Future of S&T: Implications for Intelligence* [U//FOUO], June 2006.

8. (U//~~FOUO~~) Intelligence Science Board Report on *The State of Science and Technology Analysis in the Intelligence Community* [redacted] April 2004.

9. (U//~~FOUO~~) Intelligence Science Board Report on *The Challenge of the New S&T Landscape* [U//FOUO], November 2006.

10. (U//FOUO) Director of National Intelligence, *The National Cyber Initiative* [redacted], Version dated December 17, 2007.

11. (U) Defense Science Board Task Force Report on *High Performance Microchip Supply* [U], February 2005.

12. (U) Defense Science Board Task Force Report on *Mission Impact of Foreign Influence on DoD Software* [U], September 2007.

13. (U//~~FOUO~~) Committee for National Security Systems, *Framework for Mitigating Risk of Supply Chain Attacks in our Information Technology and Telecommunications Infrastructures* [U//FOUO], September 2006.

14. (U//~~FOUO~~) United States Telecommunications Infrastructure Security Study Panel Report on *Protecting the United States Telecommunications Infrastructure: The Way Forward* [U//FOUO], October 2004.

(b)(3)

15. (U) National Academy of Sciences Report on *Rising above the Gathering Storm* [U], February 2006.

16. (U) National Space INFOSEC Steering Council *Annual Assessment of the INFOSEC Status for United States Satellites and Space Systems* [redacted], October 2007.

17. (U//~~FOUO~~) CIA Report on *Information Technology Facing Security Crossroads: A Strategic Perspective* [redacted] April 2004.

18. (U) CIA Report on *Insidious Cyber Supply Chain Threat Defies Easy Solution* [redacted] August 2006.