Square Legal Pegs in Round Cyber Holes: The NSA, Lawfulness, and the Protection of Privacy Rights and Civil Liberties in Cyberspace

John N. Greer*

One of the major themes of the Cyberspace Policy Review (the Review) is that a national strategy on cybersecurity must be consistent with the protection of privacy rights and civil liberties guaranteed by the Constitution and the law.[1] Indeed, President Obama underscored that point in announcing the Review when he said that his Administration "will preserve and protect the personal privacy and civil liberties that we cherish as Americans," reiterating the theme from his inaugural address that choosing between our safety and our ideals is a false choice.[2] The authors of the Review are to be commended for encouraging a national dialogue on how this can be achieved while promoting national and economic security. Intelligence agencies, particularly the National Security Agency (NSA), are at the intersection of these vital interests, and intelligence lawyers face daunting but tremendously exciting and important opportunities to help ensure that their agencies operate in ways that effectively balance demands for both privacy and civil liberties and for the security of cyberspace.

These opportunities challenge lawyers because most of the authorities and restrictions under which intelligence agencies operate today were established in a pre-cyberspace world. The NSA, for example, for most of its nearly 60-year history operated in two distinct and separate arenas; one was primarily foreign, the other primarily domestic. In the foreign arena, the NSA focused on the collection and dissemination of foreign intelligence derived from signals intelligence (SIGINT) activities. In the domestic arena, the NSA focused on the defense and protection of sensitive national security information systems under its Information Assurance (IA) activities. The NSA's foreign and domestic arenas traditionally differed in

---

* Associate General Counsel, Information Assurance, Office of General Counsel, National Security Agency. I thank former National Security Agency General Counsel Vito Potenza, former Deputy Chief of Staff Ethan Bauman, and attorneys Maxine Mead, Cathy Owen, and Linda Brandt for their assistance in preparing this article. I would also like to acknowledge Alex Joel, Civil Liberties and Privacy Officer in the Office of the Director of National Intelligence, for developing the conceptual framework that I apply in this article.

1. CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

2. President Barack Obama, Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009), *available at* http:www.whitehouse.gov/the_press _office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ [hereinafter Remarks by the President]; President Barack Obama, Inaugural Address (Jan. 20, 2009), *available at* http://www.whitehouse.gov/blog/inaugural-address/.

many respects, including staff, oversight and compliance requirements, budgets, and authorities.

NSA lawyers inherited this bifurcated structure and are charged with applying it in today's cyberspace environment. As has often been said, communications have merged with the global digital infrastructure. The World Wide Web, as the President stated, "has made us more interconnected than at any time in human history."[3] It is no longer appropriate to think in terms of geographic boundaries between "foreign" and "domestic" activities because these concepts lose their meaning in cyberspace. The NSA's foreign intelligence collection mission and its domestic IA mission can be seen as two sides of the same coin. Knowing how foreign adversaries threaten U.S. cybersecurity helps the NSA develop appropriate defensive measures, and knowing how those measures work helps the NSA understand the threats posed by its adversaries.

This article explores issues raised by the need to interpret pre-cyberspace legal authorities and restrictions in a cyberspace world, and how that is done in a way that protects privacy and civil liberties.[4] SIGINT authorities and restrictions, for instance, were developed to protect the privacy rights of U.S. persons[5] whose communications were intentionally targeted to obtain foreign intelligence, requiring a court order under the FISA,[6] or were incidentally collected while targeting foreigners overseas to obtain foreign intelligence. The latter situations require "minimization" under procedures approved by the U.S. Attorney General in order to protect the identities of U.S. persons except where necessary to understand or assess the foreign intelligence. What authorities and restrictions apply when foreign intelligence is obtained by associating foreign methods of computer intrusion with U.S. Internet Protocol addresses? How would minimization of U.S. identities work in a cybersecurity network where information is shared in real time?

Or consider the scenario in which the NSA sees a massive foreign cyber intrusion aimed at the U.S. banking system. The NSA has the authority to support the efforts of the Department of Defense (DoD) to protect its networks. The NSA also has authority to provide technical cybersecurity assistance to other federal departments and agencies so that they can protect their networks.[7] However, the NSA is not authorized to

---

3. Innaugural Address, *supra* note 2.

4. This article was written before the Secretary of Defense decided on June 23, 2009, to establish the United States Cyber Command, and therefore it does not address the legal implications of that decision.

5. The term "U.S. person" generally includes citizens of the United States, permanent resident aliens, unincorporated associations substantially composed of U.S. citizens or permanent resident aliens, and corporations that are incorporated in the United States, except for corporations directed and controlled by foreign governments.

6. 50 U.S.C. §1801 (2006).

7. Executive Order No. 12,333 (as amended), *United States Intelligence Activities*, 73 Fed. Reg. 45,325 (July 30, 2008).

assist operators of private sector critical infrastructure systems directly. Thus, a key question is under what authorities and restrictions may the NSA act to see and prevent computer intrusions – at cyberspeed – so that the banking system is not shut down and the country's economy is not brought to a halt.

The way for the NSA to meet these security challenges and also allay concerns about civil liberties violations is for the U.S. government and the NSA in particular to earn and maintain the trust of the American people. This can best be accomplished in three ways: by maintaining transparency, by continuing oversight, and by establishing clarity of roles and missions. This article examines each in turn, but first comments on intelligence agency roles, as discussed in the Review.

I. INTELLIGENCE AGENCIES PLAY A CRITICAL ROLE IN CYBERSECURITY

No one disputes that intelligence agencies play a critical role in cybersecurity. The Review recommends that the federal government "should continue to leverage the nation's long-term investments in the fundamental development of cryptologic and IA technologies and the necessary supporting infrastructure."[8] By "leverage," the Review means the ability of the federal government to take advantage in the cybersecurity area of investments made in another area – that is, the investments Congress has funded in cryptology and IA.

Leveraging those investments will result in enhanced information sharing between the NSA and other parts of the federal government responsible for cybersecurity, and that will, in turn, promote the Review's goal of improving the nation's cybersecurity posture. This is the principle behind "mission bridging" that the Review cites with approval as having begun in the last President's administration under the Comprehensive National Cybersecurity Initiative (CNCI).[9] The Review recommends that mission bridging continue and be expanded. "Departments and agencies should expand the sharing of expertise, knowledge, and perspectives about threats, tradecraft, technology, and vulnerabilities between network defenders and the intelligence, military, and law enforcement organizations that develop U.S. operational capabilities in cyberspace."[10]

II. BALANCING PRIVACY AND CIVIL LIBERTIES WITH SECURITY

The task is how to expand the sharing of cybersecurity information when intelligence agencies are involved while protecting privacy rights and civil liberties. Many people are rightly concerned when they hear that

8. CYBERSPACE POLICY REVIEW, *supra* note 1, at 29.
9. *Id.* at 8.
10. *Id.*

intelligence agencies will be more active in cyberspace. In general, the American public is highly suspicious of concentrations of power and secrecy, particularly in institutions that exhibit both.

The NSA is such an institution. It has considerable technical electronic surveillance capabilities and, to be effective, it must largely operate out of the public eye so that adversaries will not change their methods in undetectable ways. With respect to privacy and civil liberties, many critics have argued that the NSA overstepped its bounds and subverted the congressional oversight process after the attacks of September 11, 2001, by conducting warrantless surveillance against Americans and limiting knowledge of these activities to only a few members of Congress.[11] The Director of the NSA, Lieutenant General Keith B. Alexander, recognizes that this perception exists and recently laid down a challenge that is highly relevant to lawyers in the intelligence community advising clients operating in cyberspace: "As you walk through cybersecurity, you get the impression that it is civil liberties or security. I think we've got to endeavor to do both. Equally and balance them. We do. For all of us."[12]

A. Transparency

Transparency means that intelligence agencies like the NSA must explain what they do as openly and as candidly as possible. There may be some aspects, however, such as sensitive sources and methods, that cannot be fully discussed in public lest foreign adversaries learn too much about how to defeat U.S. efforts. With respect to cybersecurity under the CNCI, the classified nature of much of the CNCI limited public discussion. The Review, on the other hand, will facilitate such discussion, including about the role of intelligence agencies. Lieutenant General Alexander made important contributions to this discussion through recent public statements[13] about the need to:

- Match federal capabilities with authorities.
- Establish a "common operating picture."
- Share cybersecurity information in real time and broadly.

---

11. *See, e.g.,* Ellen Nakashima, *House Bill Expands Oversight of NSA*, WASH. POST, June 20, 2009, at A13.

12. Lieutenant General Keith B. Alexander, Director, NSA, Remarks at RSA Conference, San Francisco (Apr. 21, 2009), *available at* http://www.nsa.gov/public_info/speeches_testimonies/21apr09_dir.shtml.

13. *Id. See also Cyberspace as a Warfighting Domain: Policy, Management, and Technical Challenges to Mission Assurance: Hearing Before the H. Armed Serv. Subcomm. on Terrorism, Unconventional Threats and Capabilities,* 111th Cong. 1 (May 5, 2009) [hereinafter Hearing] (statement of Lieutenant General Alexander), *available at* http://armedservices.house.gov/pdfs/TUTC050509/Alexander_Testimony050509.pdf.

These three challenges, identified by Lieutenant General Alexander, are discussed in detail here.

1. The Need To Match Capabilities with Authorities

Lieutenant General Alexander noted that the NSA has the world's center of gravity for crypto-mathematicians and should take advantage of that fact for the good of the nation.[14] The NSA, he said, has brought its unique defensive and collection capabilities together in the form of the NSA/Central Security Service Threat Operations Center. Arrangements like this permit a "defense-in-depth" approach that would be particularly effective against a distributed denial-of-service attack where the NSA's defensive and collection missions can partner to stop these attacks.[15] While there are a number of ongoing policy issues related to the question of how best to organize the federal government to achieve this goal, the issue for NSA lawyers will be to ensure that any such activity is conducted in accordance with all applicable laws, policies, and procedures and is properly authorized.

The NSA's defense mission is carried out chiefly through its IA activities. NSA lawyers need to be sure that the agency's IA computer monitoring operations are conducted in strict conformity with the following laws (among others):

- Fourth Amendment to the Constitution[16]
- Federal Wiretap Act[17]
- Pen Registers and Trap and Trace Devices chapter of Title 18[18]
- Computer Fraud and Abuse Act[19]

---

14. Remarks at RSA Conference, *supra* note 12.

15. *Hearing, supra* note 13. For more on the IA strategy of "defense-in-depth," see Keith B. Alexander, *Secure from the Start: Designing and Implementing an Assured National Security Enterprise*, CROSSTALK: JOURNAL OF DEFENSE. SOFTWARE ENGINEERING, *available at* http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA488206& Location=U2&doc =GetTRDoc.pdf.

16. U.S. CONST. amend. IV.

17. 18 U.S.C. §§2510-2522 (2006). This law was first passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (and is generally known as "Title III"). *See generally* U.S. DEPARTMENT OF JUSTICE, COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION, CRIMINAL DIVISION, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE MANUAL, at CH. 4 (Electronic Surveillance in Communications Networks) (2009), *available at* http://www.cybercrime.gov/ssmanual/04ssma.pdf.

18. 18 U.S.C. §§3121-3127 (2006). Known as the "Pen/Trap statute," this statute was first passed as part of the Electronic Communications Privacy Act of 1986. *See generally* U.S. DEPARTMENT OF JUSTICE, *supra* note 17.

19. 18 U.S.C. §1030 (2008). *See generally* U.S. Department of Justice, *supra* note 17, at ch. 1.

- Computer Security Act of 1987[20]

Moreover, the NSA may not monitor computer networks for IA purposes without having received formal requests for assistance from their owners or service providers. NSA lawyers also need to be sure that agency IA activities are properly authorized. The NSA helps protect the worldwide computer networks of the DoD and national security systems[21] pursuant to a variety of legal authorities.

a. National Security Directive 42

One of the primary sources of the NSA's "defense" authority is National Security Directive (NSD) 42.[22] President George H. W. Bush recognized that ensuring the security of national security systems is vitally important to the operational effectiveness of the activities of the government and to military combat readiness. Therefore, he directed that government capabilities for securing national security systems against technical exploitation threats be maintained or improved to provide for reliable and continuing assessment of threats and vulnerabilities and for the implementation of effective countermeasures. The President stated that as a policy, government and contractor national security systems shall be secured by such means as necessary to prevent compromise, denial, or exploitation.

To implement this objective and policy, the President created the Policy Coordinating Committee under the National Security Council and established the Committee on National Security Systems (CNSS) to oversee the implementation in this area.[23] The CNSS today provides a forum for

---

20. Pub. L. No. 100-235, 101 Stat. 1724 (1988) (codified as amended at 15 U.S.C. §§272, 278g-3, 278g-4).

21. "The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency–(i) the function, operation, or use of which (I) involves intelligence activities; (II) involves cryptologic activities related to national security; (III) involves command and control of military forces; (IV) involves equipment that is an integral part of a weapon or weapons system; or (V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or (ii) 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." 44 U.S.C. §§3542(b)(2)(A) (2002). "Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications)." 44 U.S.C. §§3542(b)(2)(B) (2002).

22. NATIONAL POLICY FOR THE SECURITY OF NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS, July 5, 1990. Partial text version of NSD 42 was released under a Freedom of Information Act request of September 13, 1990 and is *available at* http://www.fas.org/irp/offdocs/nsd/nsd_42.htm.

23. In NSD 42, the President established an interagency group at the operating level called the National Security Telecommunications and Information Systems Security

discussion of policy issues, sets national policy, and promulgates direction, operational procedures, and guidance for the security of national security systems. The CNSS is chaired by the Department of Defense.

Further, the President named the Secretary of Defense as the Executive Agent of the government authorized to protect national security systems and the Director of the NSA as the National Manager.[24] In July 2008, the President amended Executive Order (EO) 12,333, and, while he retained the Director as National Manager, he made him responsible in this capacity to the Director of National Intelligence as well as to the Secretary of Defense.[25] An issue that needs to be examined is whether, to enhance protection of national security systems, the CNSS and the National Manager should have clearer authority to enforce their decisions.

The NSA has considerable expertise in protecting sensitive networks. This is recognized in NSD 42. Under this authority, the NSA may provide technical assistance to owners of national security systems (i.e., to the government and to government contractors) and conduct vulnerability assessments of those systems. Among other things, NSD 42 also requires the NSA to disseminate information on threats to and vulnerabilities of national security systems.

b. Executive Order 12,333

Subsections 2.6(c) and (d) of Executive Order 12,333 permit the NSA and other intelligence agencies to provide specialized equipment, technical knowledge, and assistance of expert personnel for use by any department or agency and render any other assistance and cooperation to civil authorities not precluded by law. The NSA's provision of assistance of expert personnel must be approved in each case by the NSA General Counsel. This authority applies to the provision of NSA assistance to owners of both national security systems and non-national security systems.[26]

c. Statutory and Regulatory Authority for the DoD's IA Program

The National Defense Authorization Act for Fiscal Year 2000 directed the Secretary of Defense to carry out an IA program "to protect and defend Department of Defense information, information systems, and information networks that are critical to the Department and the armed forces during

---

Committee (NSTISSC) to consider technical matters and develop operating policies, guidelines, instruction, and directives as necessary to implement the provisions of NSD 42 Section 5. Then in EO 13,231, "Critical Infrastructure Protection in the Information Age," the President redesignated the NSTISSC as the CNSS. Exec. Order No. 13,231, 66 Fed. Reg. 53,063 (Oct. 16, 2001).

24. NSD 42, *supra* note 22, at §§6,7.

25. Exec. Order No. 12,333, *supra* note 7, at §1.7(c)(6).

26. *Id.*

day-to-day operations and in operations in times of crisis."[27] The objectives of the program are "to provide continuously for the availability, integrity, authentication, confidentiality, nonrepudiation, and rapid restitution of information and information systems that are essential elements of the Defense Information Infrastructure."[28] Pursuant to this statutory authority, the DoD has issued regulatory guidance. In DoD Directive 8500.01E, for example, the Deputy Secretary of Defense, Paul Wolfowitz, stated as DoD policy that DoD information systems:

> shall be monitored based on the assigned mission assurance category and assessed risk in order to detect, isolate, and react to intrusions, disruption of services, or other incidents that threaten the IA of DoD operations or IT resources, including internal misuse. DoD information systems shall also be subject to active penetrations and other forms of testing used to complement monitoring activities in accordance with DoD and Component policy and restrictions.[29]

d. Multiple Lines of Authority for National Security Systems

In 2008, the Secretary of Defense directed the Commander of the United States Strategic Command to place the DoD's Joint Task Force-Global Network Operations (JTF-GNO) under the operations control of the Commander of the Joint Functional Component Command-Network Warfare. The individual assigned as Commander of the Joint Functional Component Command-Network Warfare (JFCC-NW) is also assigned as the Director of the NSA. This construct means that the security arrangements for national security systems recognize that authority for protecting national security systems may flow through one officer who is simultaneously assigned as: (1) Commander of the JFCC-NW (the authorities of Commander, the Joint Functional Component Command-Network Warfare are exercised via and under the Commander of the United States Strategic Command); (2) Director of the NSA; and (3) National Manager for national security systems.

e. Signals Intelligence Authorities

The NSA's ability to engage in the collection of SIGINT data is a tool often used to support the NSA's computer network defense mission. The NSA is authorized by Executive Order 12,333 to conduct SIGINT activities, including data collection, only for the purposes of foreign

27. 10 U.S.C. §2224(a) (2006).

28. *Id.* §2224(b) (200§2224(b).

29. U.S. DEP'T OF DEFENSE, DIR. 8500.01E, INFORMATION ASSURANCE 7 (2002), *available at* http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf.

intelligence, counterintelligence, and support for military operations.[30] The NSA's SIGINT activities are conducted in strict conformity with, among other laws, the Fourth Amendment, the Foreign Intelligence Surveillance Act (FISA) of 1978, and the FISA of 1978 Amendments Act of 2008 (FISA Amendments).[31] The NSA conducts SIGINT collection based on the foreign intelligence requirements of government customers. These requirements may include topics related to cybersecurity.

2. Need for a "Common Operating Picture"

Lieutenant General Alexander has also highlighted the need to establish what the Review calls a "common operating picture."[32] There is a need for a center to gather information from multiple sources and establish a comprehensive view of the health of the global digital network. Such sources include: U.S. federal, state, local, and tribal governments; foreign governments; and private organizations. Only with this type of awareness can assessments be made about what is happening in cyberspace at any given moment. Such an arrangement raises a host of legal questions, such as how to make information available to those staffing such a center while complying with restrictions placed on data provided by private organizations or foreign governments, particularly European restrictions treating Internet Protocol addresses as protected personal information.[33] Policies and procedures need to be developed that will permit critical infrastructure entities to share cybersecurity threat information with the federal government in real time and in a way that protects proprietary and otherwise privileged information. Mechanisms could be developed to "tag" each data element with attributes such as the authorities and restrictions under which the data were provided.

Access to data will need to be limited to those with proper authority. If voluntary sharing is not feasible or practicable, it may be appropriate to consider a regulatory approach under which owners of critical infrastructure are required to keep standardized cybersecurity information about threats and the health of their systems and share it with the federal government in a real time, ongoing manner or, alternatively, upon some triggering event.

---

30. Exec. Order No. 12,333, *supra* note 7, at §1.7(c).

31. Pub. L. No. 110-261, 122 Stat. 2436 (2008).

32. CYBERSPACE POLICY REVIEW, *supra* note 1, at 5.

33. *See, e.g.*, Council Directive 95/46, 1995 O.J. (281) 31 (EC), *available at* ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf; Council Directive 2002/58, 2002 O.J. (201) 37 (euratom), *available at* eur-lex.europa.eu/LexUri Serv/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML.

3. Need To Share in Real Time and Broadly

As Lieutenant General Alexander has noted, there is a need to find a way to share cybersecurity information in real time at network speed.[34] It is not sufficient in today's networking world merely to note after the fact that an intrusion has occurred. One must see malicious activity and warn others as it is happening so that appropriate actions can be taken. Because many of these responses necessarily must be automated and programmed ahead of time, lawyers in the Intelligence Community will need to understand the response mechanisms and ensure that the computer program triggering those responses does so in legal ways.

Communications and information systems are rapidly converging onto the same digital network.[35] This fact necessitates sharing cybersecurity information so that those responsible for defending their respective systems, such as federal departments and agencies outside the DoD and the Intelligence Community, U.S. allies, and the U.S. private sector can take action.[36] A major issue for intelligence operators is finding a way to share cybersecurity information that may have been collected from sensitive sources without disclosing information that must remain secret. Lawyers advising these intelligence operators must make sure that the sharing is consistent with the protection of privacy rights and civil liberties in accordance with applicable laws, policies, and procedures.

This section examines information sharing within the government; sharing of information between the government and the private sector is discussed below under "Clarity of Roles and Missions."

When the classified information in question is the SIGINT or IA information of the NSA, certain legal restrictions on sharing apply. SIGINT must be shared within the framework of the legal constraints related to information privacy rights and safeguarding classified information. Executive Order 12,333 specifically notes that SIGINT is not to be shared as freely as other types of intelligence information. Section 2.3(j) states that:

> . . . agencies within the Intelligence Community may disseminate information, other than information derived from signals intelligence, to each appropriate agency within the Intelligence Community for purposes of allowing the recipient agency to determine whether the information is relevant to its responsibilities and can be retained by it, *except that information derived from signals intelligence may only be disseminated or made available to Intelligence Community elements in accordance with procedures established by the Director [of National Intelligence] in*

34. Remarks at RSA Conference, *supra* note 12.

35. *Id.*

36. CYBERSPACE POLICY REVIEW, *supra* note 1, at 4.

> *coordination with the Secretary of Defense and approved by the Attorney General."* [37]

Guidelines currently in effect require that the NSA may not simply provide SIGINT to customer agencies in order for those agencies to determine whether the SIGNT is helpful to them. Instead, before disseminating the information, the NSA must assess the information to determine whether it has foreign intelligence value. It must also minimize information from U.S. individuals unless it reveals that that information is necessary to understand the foreign intelligence information.

The NSA's dissemination procedures, approved by the Attorney General, are designed to recognize and address the constitutional dimensions of SIGINT collection.[38] SIGINT is an intrusive form of intelligence gathering, and SIGINT activities must be carried out in a manner that is "reasonable" under the Fourth Amendment.[39] The Fourth Amendment protects all U.S. persons anywhere in the world and all persons within the United States from unreasonable searches and seizures by any person or agency acting on behalf of the U.S. government.

The Supreme Court has ruled that interception of electronic communications in which there is a reasonable expectation of privacy is a search and seizure within the meaning of the Fourth Amendment.[40] It is therefore mandatory that SIGINT operations be conducted pursuant to procedures that meet the reasonableness requirements of the Fourth Amendment, balancing the U.S. government's need for foreign intelligence information with the information privacy interests of persons protected by the Fourth Amendment. Thus, SIGINT may only be disseminated after it has been evaluated for foreign intelligence and reviewed for minimization purposes under NSA procedures.

In addition, information collected under an order of the Foreign Intelligence Surveillance Court (FISC) may be disseminated only in accordance with the minimization procedures approved by the court.[41] These minimization procedures must be applied to the data prior to dissemination.

As we move forward in the cyberworld with its demand for increased information sharing, it may be appropriate to seek approval from the FISC

---

37. Exec. Order No. 12,333, *supra* note 7, at §2.3(j) (emphasis added).

38. The procedures are based on the DoD Regulation 5240.1-R classified annex and consolidated in NSA's United States Signals Intelligence Directive 18, which is *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index2.html.

39. *See generally* Michael Hayden, *Balancing Security and Liberty: The Challenge of Sharing Foreign Signals Intelligence*, 19 NOTRE DAME J.L. ETHICS & PUB. POL'Y 247 (2005).

40. *See, e.g.*, Berger v. New York, 388 U.S. 41, 51 (1967); Katz v. United States, 389 U.S. 347, 353 (1967).

41. 50 U.S.C.A. §1806 (West 2003 & Supp. 2009).

of amended minimization procedures so that anyone conducting a SIGINT mission under the authority, direction, or control of the Director of the NSA may have access to unminimized FISA collection, to include collection under the FISA Amendments Act.

For both SIGINT and IA information, the NSA and other DoD intelligence agencies must comply with DoD Regulation 5240.1-R's restrictions on the dissemination of information about U.S. persons.[42] As a general rule, U.S. persons must consent to the monitoring of their communications as a condition of any subsequent dissemination pursuant to DoD regulations.[43] If that consent has been obtained, U.S. person information may be shared with the following recipients if it is reasonably believed that such recipients need the information to perform a lawful government function: (1) DoD employees or contractors who need the information in the course of official duties; (2) federal, state, or local law enforcement organizations if the information indicates activities that may violate laws within their respective jurisdictions; (3) with certain caveats, other Intelligence Community agencies; or (4) federal government agencies authorized to receive the U.S. person information in the performance of a lawful government function.[44] Proposed NSA disseminations that do not fall into any of these categories must be approved by the NSA Office of General Counsel after consultation with the Department of Justice and DoD General Counsel.[45]

A set of procedures approved by the Attorney General known as National Telecommunications and Information Systems Security Directive (NTISSD) 600 covers communications security (COMSEC) monitoring.[46] COMSEC monitoring directly implicates the Fourth Amendment and is potentially highly intrusive because it involves the monitoring of the communications of U.S. persons for communications security purposes. NTISSD 600 spells out that heads of departments or agencies (or in the case of government contractors, the chief executive officer), or their designees, operating systems to be monitored must request COMSEC services and certify to the Director of the NSA that their organizations have implemented programs that give users legally sufficient notice of monitoring.[47] NTISSD 600 strictly regulates the dissemination of information about U.S. persons in order to protect their privacy rights.

The procedures in DoD Regulation 5240.1-R and NTISSD 600 also help to ensure that monitoring activities undertaken for IA purposes are not illegal

---

42. U.S. DEP'T OF DEFENSE, Reg. 5240.1-R, PROCEDURES GOVERNING THE ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS (Dec. 1982).

43. *Id.* at 7.

44. *Id.* at 22-23.

45. *Id.* at 23.

46. "Communications Security (COMSEC) Monitoring," National Telecommunications and Information Systems Security, April 10, 1990.

47. NTISSD 600, §§14, 31d.

under the Federal Wiretap Act.[48] It is not unlawful, for instance, for the federal government to intercept the communications of executive branch entities or contractors for communications security purposes under procedures approved by the Attorney General.[49] It is also not unlawful, under federal law, to intercept a communication when a party has given prior consent.[50] (The government party is considered to be the consenting party.) Finally, it is not unlawful for employees of providers of wire or electronic communications to intercept, disclose, or use a communication in the normal course of employment while engaged in any activity that is a necessary incident to the rendition of service or to the protection of the rights and property of the provider.[51] This "service provider" exception is routinely used by the operators of DoD systems (such as the Defense Information Security Agency and the JTF-GNO) and by the NSA's IA personnel operating under DoD service provider authority.

B. Oversight

The second way of earning and maintaining the trust of the American people is to demonstrate that intelligence agencies operate within an effective oversight system. "To keep the people's trust, NSA and other intelligence agencies must be extremely careful to follow rules that have been laid down by elected representatives in the legislative and executive branches, as well as by the courts."[52] As a former Director of the NSA put it:

> The American people must be confident that the power they have entrusted to NSA is not being, and will not be, abused. The resulting tension–between secrecy on one hand and open debate on the other–is best reconciled through rigorous oversight. It serves as a needed check on what has the potential to be an intrusive system of intelligence gathering. The oversight structure, in place now for nearly a quarter of a century, has ensured that the imperatives of national security are consistent with democratic values. United States intelligence today is a highly regulated activity and properly so.[53]

NSA cybersecurity activities are subject to an exhaustive oversight and compliance system, both internally and externally. Internally, this includes component oversight and compliance officers, component-level training, reviews by the Offices of General Counsel and Inspector General, and an

48. 18 U.S.C. §§2510-2522 (2006 & Supp. II 2008).
49. *Id.* §2510.
50. *Id.* §2511(2)(c).
51. *Id.* §2511(2)(a)(i).
52. Hayden, *supra* note 39, at 251.
53. *Id.*

Agency Privacy and Civil Liberties officer.[54] Across the Executive Branch, NSA activities are subject to review by the Department of Justice, the Intelligence Oversight Board, the Office of the Director of National Intelligence Civil Liberties Protection Officer, and the Privacy and Civil Liberties Oversight Board. In addition, the Armed Services, Intelligence, Judiciary, and Government Reform Committees of Congress conduct oversight. By reviewing applications to the FISC, the Judicial Branch also exercises oversight.

C. Clarity of Roles and Missions

The third way to earn and maintain trust is to explain to the American people that intelligence agencies operate within clearly defined roles and that these agencies understand the limits of these roles. Lieutenant General Alexander explained recently that the NSA's job in cybersecurity is to serve as part of a team.[55]

Currently, the NSA has an effective partnership with the defense and intelligence communities and uses its technical capabilities to help protect their networks and, as discussed above, is authorized under NSD 42, Executive Order 12,333, and DoD regulations to do so. Beyond that, the NSA is not seeking any greater authority to secure federal networks outside the DoD and the Intelligence Community, which is properly the responsibility of the Department of Homeland Security (DHS).[56] Rather, the NSA understands that its job is to provide technical support to the DHS, and Lieutenant General Alexander has said so publicly.[57]

The job for NSA lawyers is to ensure that the agency is authorized to provide this technical assistance to the DHS and other federal agencies for the purpose of helping them defend networks that are not national security networks. As mentioned, the NSA is authorized to provide technical assistance, including providing information and hands-on operational assistance, to federal departments and agencies for non-national security systems pursuant to Executive Order 12,333.[58] Any assistance involving

54. *See generally* Hayden, *supra* note 39.

55. Remarks at RSA Conference, *supra* note 12.

56. *Id.*

57. *Id.*

58. With respect to systems outside the national security sector, the Computer Security Act of 1987 requires that the Commerce Department's National Institute of Standards and Technology (NIST) consult with several agencies, including the NSA, when developing standards and guidelines for non-national security systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. Nothing in the Computer Security Act of 1987 expressly precludes the NSA from providing security support to federal departments and agencies outside the national security sector. Indeed, by a Memorandum of Understanding dated March 1989, the NIST and the NSA agreed that the NSA could – upon request by federal agencies, their contractors, and other government-sponsored entities – conduct assessments of the hostile intelligence threat to federal information systems, provide technical assistance, and recommend products and solutions to

computer monitoring, again, must be conducted in accordance with relevant laws, policies, and procedures. Depending on the nature of the technical assistance, this may require that the NSA's proposed assistance be approved based on the following criteria defined to establish compliance with the Federal Wiretap Act's service provider and consent provisions. Specifically, compliance may be established if: (1) the NSA's actions are a necessary incident to the rendition of service or to the protection of the entity's rights or property as a service provider, (2) the users of the entity's systems have given legally sufficient consent to monitoring of their communications, or (3) both conditions apply

The NSA's authority to provide IA assistance directly to the U.S. private sector raises difficult legal questions. The NSA has no express authority under current law or policy to provide direct IA operational assistance, including disseminating automated data collected from attack detection and warning sensors or giving tools derived from such information to the private sector. The NSA may, however, provide indirect support. It may assist the DHS (or a critical infrastructure sector-specific agency (SSA) designated under Homeland Security Policy Directive 7.[59]) The NSA may provide indirect IA assistance to private sector critical infrastructure entities only in specific ways. First, the NSA may respond to an explicit request by the DHS or the SSA that the NSA help the DHS or the SSA to help a private entity. Second, the NSA may assist if the NSA operates under the direct supervision of and pursuant to the control of DHS or the SSA. Third, NSA assistance may occur to the extent that the DHS or SSA requests such assistance. Documenting these legal relationships can be awkward and time consuming.

As the Review notes, a better way needs to be found to bring the capabilities of the federal government to bear on protecting the nation's private critical infrastructure and key resources. For example, authorities might need to be clarified and policies and procedures might need to be developed for the NSA to share cybersecurity threat information and protection measures directly with owners of critical infrastructure or their service providers in a manner that does not violate prohibitions on preferential treatment or conducting economic espionage. The legal implications of a voluntary program for the exchange of cybersecurity threat information between the government and private electronic communication service providers need to be explored.

---

secure systems against the threat.

59. DEP'T HOMELAND SEC., DIR. 7, CRITICAL INFRASTRUCTURE IDENTIFICATION, PRIORITIZATION, AND PROTECTION (2003), *available at* http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm.

CONCLUSION

The Review has it right that government cybersecurity measures must take into account U.S. privacy rights and civil liberties. Intelligence agencies today, including the NSA, operate in a highly regulated environment designed to ensure the proper balance of privacy and civil liberties with security. This is accomplished through transparency, oversight, compliance, and clarity of roles and missions. This framework is intended to provide the American public with confidence that core democratic values will be respected as the country moves to assure its safety in cyberspace. Americans want to know that their computers will not be hacked into, that their financial transactions online are safe, that they have freedom of expression on the Internet, and that they can petition their government electronically for redress of grievances. Ultimately, securing Americans' communications in cyberspace *is* protecting their privacy and safeguarding their fundamental civil liberties.