RECOMMENDATIONS FOR THE IMPLEMENTATION OF A COMPREHENSIVE AND CONSTITUTIONAL CYBERSECURITY POLICY

A REPORT BY THE CONSTITUTION PROJECT'S LIBERTY AND SECURITY COMMITTEE

January 27, 2012

The Constitution Project
1200 18th Street, N.W.
Suite 1000
Washington, D.C. 20036
202.580.6920 (tel)
202.580.6929 (fax)
info@constitutionproject.org

www.constitutionproject.org

RECOMMENDATIONS FOR THE IMPLEMENTATION OF A COMPREHENSIVE AND CONSTITUTIONAL CYBERSECURITY POLICY

I. INTRODUCTION

The risk of pervasive and sustained cyber-attacks against the United States with potentially devastating effects on federal computer systems and operations as well as on networks that control critical civilian infrastructure,[1] must be effectively addressed in a manner that protects constitutional rights. In this increasingly interconnected era, computer-induced failures of U.S. power-grids, transportation networks, or financial systems could cause both physical damage and economic disruption.[2] Our intermeshed private and government computing infrastructure includes telecommunications and wireless networks, technologies that carry data and multimedia communications, and control systems for our power energy distribution, transportation, and manufacturing.[3] As the nation harnesses the power of computer networks to create and share knowledge, and produce economic goods, it is also developing new vulnerabilities to those who would steal, corrupt, harm, or destroy public and private assets that are vital to our national interests.[4]

It is important that our nation develop and operate cybersecurity programs and policies to reduce or eliminate these vulnerabilities. These programs, however, pose a potential threat to Americans' privacy rights and civil liberties. As proposals have arisen that would enable the federal government to move toward monitoring all information transferred over private networks, individuals face the risk of being subjected to the equivalent of a perpetual "wiretap" on their private communications and web browsing behavior. Moreover, the debate regarding cybersecurity has been hampered by excessive secrecy surrounding the true nature and scope of the threat and the best mechanisms for protecting against it.

The security of our nation's computer networks is critical not only to the government and businesses, but also to the growing number of individual Americans who rely on the internet in their daily lives. Americans today use the internet for a broad range of activities, from banking and paying bills to obtaining news and entertainment programming to correspondence and social networking. According to the most recent Census, nearly 70 percent of all Americans used the

---

[1] Gregory C. Wilshusen, Director, Information Security Issues and David A. Powner, Director, Information Technology Management Issues, United States Government Accountability Office, Statement for the Record to the Subcommittee on Terrorism and Homeland Security, Committee on the Judiciary, United States Senate, Nov. 17, 2009, p. 1; William J. Lynn III, "Defending a New Domain," *available at* http://www.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx, p. 2; James R. Clapper, Director of National Intelligence, "Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community for the House Permanent Select Committee on Intelligence," Feb. 10, 2011, at 27.

[2] James R. Clapper, Director of National Intelligence, "Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community for the House Permanent Select Committee on Intelligence," Feb. 10, 2011, at 27.

[3] *Id*. at 26-27.

[4] *Id*. at 27.

internet in their homes in 2009.[5] This figure is certain to grow as businesses and governments at all levels seek to extend high-speed access to every pocket of the country. The pervasiveness of the internet – and the willingness and need of so many Americans to share sensitive personal and financial information online – is forcing policymakers to grapple with how to extend Fourth Amendment guarantees to the digital world.

For these reasons and as outlined further below, we, the undersigned members of The Constitution Project's bipartisan Liberty and Security Committee, recommend that critical safeguards be incorporated into current and future government cybersecurity programs to ensure protection for fundamental constitutional rights. This report concludes with our recommendations for safeguards to be incorporated into any government cybersecurity policy.

A. BACKGROUND

In 2008, President George W. Bush launched the Comprehensive National Cybersecurity Initiative ("CNCI") to strengthen and protect the federal computer network from cyber threats. The Obama administration, also recognizing the dangers posed by cyber-attacks, has continued to implement and expand the CNCI.[6] A key part of the CNCI is a set of cybersecurity technologies referred to as "Einstein," first introduced in 2003. Einstein's purpose is to detect and help eliminate harmful activity from the federal computer network.

Einstein's latest two iterations, Einstein 2 (deployed) and Einstein 3 (currently in field-testing) have advanced capabilities to examine and archive a vast amount of communications between federal agencies and their employees and with the public. The United States Computer Emergency Readiness Team ("US-CERT"), a branch of the Department of Homeland Security ("DHS"),[7] retains and may review communications that Einstein flags as possible threats. While Einstein's capabilities are laudable in helping secure government information systems, these cybersecurity tools also raise significant Fourth Amendment concerns.

Specifically, the Einstein program has raised concerns about whether DHS and US-CERT are infringing the Fourth Amendment rights of government employees and private citizens who communicate with those federal agencies. The government review of these communications includes:

- Conducting automated inspections of all communications between federal agencies and the internet to determine if any are related to a cyber-attack;

---

[5] Source: U.S. Census Bureau, Current Population Survey, October 1984, 1989, 1993, 1997, 2000, 2001, 2003, 2007, 2009. Appendix Table A. Households With a Computer and Internet Use: 1984 to 2009.

[6] In Department of Homeland Security ("DHS") parlance, a cyber threat is "any identified effort directed toward access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, and application, or a federal system, without lawful authority." U.S. Dep't of Homeland Security, *Privacy Impact Assessment for the Initiative Three Exercise* (2010) (hereafter "Einstein PIA 3") at 3.

[7] *See* U.S. Dep't of Homeland Security, *Privacy Impact Assessment for the Einstein Program* (2004) (hereafter "Einstein PIA 1") at 3. The Einstein program is managed by US-CERT, a partnership between the National Cybersecurity Division ("NCSD") of DHS and the public and private sectors. Within DHS, the NCSD carries the primary responsibility for cybersecurity coordination and readiness. US-CERT is the main operational arm of the NCSD.

- Allowing US-CERT to save and later analyze communications suspected of being related to a cyber-attack; and

- Allowing US-CERT to share the content of suspect communications with other law enforcement or intelligence agencies.

US-CERT and the Justice Department's Office of Legal Counsel ("OLC") have stated that the information monitored and collected through Einstein, including personally identifiable information ("PII"),[8] will not be abused and that it will be collected with the consent of all monitored federal employees. The current regulations, however, are unclear. They lack identifiable safeguards to prevent stored, private information from being shared among federal agencies and possibly transferred to law enforcement agencies and used against individuals in unrelated criminal proceedings.[9]

These concerns are now heightened as Congress seeks to expand the national cybersecurity initiative (and with it the Einstein program and/or other federal cybersecurity programs) to monitor and protect critical private industry networks. The goal is to cover networks that, if attacked, would result in a "debilitating impact on … national economic security and national public health or safety."[10] These critical industries include transportation, energy, essential natural resources, health care, communications, and financial markets. Until very recently, expanding the jurisdiction of Einstein and other cybersecurity technologies so deeply into the daily lives of Americans has not been publicly discussed. Yet, now pending in Congress are bills that could permit all network communications with banks, hospitals, airlines, and other critical private industries – including personal, private communications accessed or sent across those industry networks – to be shared with the federal government as a matter of course.[11] The further the reach of federal cybersecurity programs, the greater the possible government intrusion into individuals' private communications.

B. IMPLICATIONS OF CYBERSECURITY INITIATIVES ON FOURTH AMENDMENT RIGHTS

The Einstein cybersecurity program is presently limited to traffic to and from federal agencies' computers. The OLC has formally stated that federal employees using government networks, as well as private citizens who communicate with federal agencies and their

[8] Personally Identifiable Information is defined as "information which can be used to distinguish or trace an individual's identity, … alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual … " *See* Office of Management and Budget, *Memorandum for the Heads of Executive Departments and Agencies: Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007) at 1 n.1.

[9] The *Privacy Compliance Review of the EINSTEIN Program*, issued by DHS on January 3, 2012, suggests that external sharing of cyber threat reports between DHS and another agency or organization requires an executed Memorandum of Agreement ("MOA") before any information can be shared. The MOAs should "outline what information the reports contain regarding the cyber threats and the limits on sharing." National Protection and Programs Directorate, *Privacy Compliance Review of the EINSTEIN Program* (2012) (hereinafter "Einstein PCR") at 6-7.

[10] The Cybersecurity Act of 2010, S. 773, 111th Congress (2010). This proposed legislation is one of many cybersecurity bills introduced in Congress since 2010.

[11] *See, e.g.*, Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. (2011).

employees, do not have a reasonable expectation of privacy in their communications and, therefore, that Einstein technology does not violate their Fourth Amendment right "to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures."[12] The OLC further argues that, even if citizens have a reasonable expectation of privacy, the government is still entitled to monitor network communications because individuals have consented.[13] Additionally, the government has a special need to review communications in the interest of national security. The OLC's conclusions, while debatable, support the legitimate government purpose of protecting federal agencies' operations, including our nation's intelligence, military, and commerce. Notwithstanding this legitimate and important government interest, to the extent that current or future cybersecurity programs involve widespread monitoring and sharing of individuals' private communications and the sensitive information contained therein, clear and enforced safeguards are needed to protect both our national security and our constitutional rights.

As discussed in further detail below, proposals that might permit expansion of government cybersecurity programs to cover private networks of vital importance to American society raise new concerns. Regardless of the government's earnest intentions, clear and proper safeguards should be implemented to prevent unrestricted government access to individuals' private information when searching network communications for harmful material. Otherwise, the federal government runs the risk of establishing a program akin to wiretapping all network users' communications. As is the case when government wiretapping is justified but a traditional warrant cannot be obtained – particularly when matters of national security are involved – procedures can still be established for judicial oversight to determine when private information should be reviewed in light of a clear and compelling government interest.

In addition, there is a risk that as the government partners more closely with private industry, sensitive personal information may be improperly or inadvertently disclosed. Although public-private partnerships may be an important component of cybersecurity programs, as outlined below, it is important to limit the amount and nature of personal information shared between the public and private sectors. In general, information should be sanitized or anonymized to remove all PII before it is shared with the government. The government should not be permitted to conduct an end-run around Fourth Amendment safeguards by relying upon private companies to monitor networks. Conversely, where it is not necessary for cybersecurity purposes for the government to disclose sensitive personal information or the content of communications in its possession to private companies, such sharing should be prohibited.

---

[12] *See* Memorandum for Fred F. Fielding, Counsel to the President, from Steven J. Bradbury, Principal Deputy Assistant Attorney General, Office of Legal Counsel, *Re: Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (EINSTEIN 2.0) to Protect Unclassified Computer Networks in the Executive Branch* (Jan 9, 2009); *see also* Memorandum for Associate Deputy Attorney General, from David J. Barron, Acting Assistant Attorney General, *Re: Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch* (Aug. 14, 2009).

[13] The OLC's assertion that federal employees have no expectation of privacy is also an overextension of existing laws. For example, many of the communications between private citizens and government employees are governed by rigorous standards set forth in the Privacy Act, including required notices of how private information is being used via the Privacy Act Systems of Records. *See, e.g.*, The Privacy Act of 1974, 5 U.S.C. § 552(a), Pub. L. No. 93-579 (1974).

For the reasons discussed further below, we believe that Congress and the executive branch should incorporate robust safeguards into the Einstein program and any additional federal cybersecurity initiatives. This report addresses the Fourth Amendment concerns raised by the application of Einstein 2 and the expected implementation of Einstein 3, while acknowledging the important function the Einstein program performs in protecting the government's computer networks and information systems. The report also details recent legislative proposals introduced in Congress and explores these efforts to expand cybersecurity programs into the private sector and centralize national cybersecurity responsibilities.

Thus, this report focuses on cybersecurity programs involving monitoring of internet traffic. We note that there are various other approaches to cybersecurity that do not involve such monitoring that are in various stages of development by the government and private sector. These include efforts to secure the supply chain and to develop a system of trusted identity authentication. We do not express any opinion on the efficacy of these various approaches. We focus on programs that involve monitoring of internet traffic because this is the approach embodied in the Einstein program as well as in pending legislation providing for sharing of information between the government and private sector, and because the monitoring approach raises particular concerns for protecting privacy rights and civil liberties. In other words, cybersecurity programs involving monitoring of internet traffic are already in use and likely to be expanded, and they raise serious constitutional concerns that we seek to address. We therefore focus on such monitoring programs, and at the conclusion of this report, we propose specific reforms to ensure that, as these national cybersecurity initiatives are undertaken, Americans' privacy rights are protected.

II. EINSTEIN: WHAT IT DOES AND HOW IT IS USED

A. EINSTEIN 1

Einstein 1 was developed in 2003 pursuant to the Homeland Security Act and other acts to gather "flow record" information for use in network traffic analysis.[14] A flow record is a record of connections made to an agency's IT systems.[15] It identifies the Internet Protocol ("IP") addresses of the computers that connect to the federal system, the federal destination IP addresses, and related data.[16] Creating flow records is akin to copying the destination and return addresses on all envelopes mailed to or from participating federal agencies.[17] Flow records do not include the content of the communications identified. For instance, the flow record of an email includes the email addresses of the sender and the recipients. The content would include the body of the email, and the subject line of the email is generally also considered to be content and not part of the flow record.[18] Einstein 1 gathered flow record data and forwarded it to US-

[14] U.S. Dep't of Homeland Security, *Privacy Impact Assessment for Einstein 2* (2008) (hereafter, "Einstein PIA 2") at 2-3.
[15] Einstein PIA 2, at 3; *see also* Einstein PIA 1, at 6-8.
[16] *Id.* This data included autonomous system numbers ("ASN"); ICMP type/code; packet length; communications protocol; sensor identification and connection status; source and destination IP address; source and destination port; TCP flag information; and timestamp and duration information.
[17] Einstein PIA 2, at 10.
[18] *See* Computer Crime and Intellectual Property Section, *Searching & Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009), *available at* http://www.cybercrime.gov/ssmanual/index.html ("The Pen/Trap statute permits law enforcement to obtain the header information of internet emails (except for the subject

CERT for detection and analysis of certain anomalies in the network traffic that were indicative of cyber threats.[19]

B. EINSTEIN 2

US-CERT began deploying Einstein 2 in 2007. All federal executive agencies are required to use Einstein 2 pursuant to a 2007 memorandum from the Office of Management and Budget ("OMB").[20] Einstein 2 incorporated Einstein 1's functionality and added intrusion detection technology. This technology detects malicious activity by inspecting communications to and from participating agencies, including their content, and attempting to match portions of the communication packet against patterns associated with known malicious activities.[21] These patterns are commonly referred to as "signatures."[22] Any signature matching data from a communication (including content) with data from a communication that is known to be malicious in nature would be considered a "malicious activity signature." All signatures identified by US-CERT are based on commercial or public computer security information, incidents reported and/or analyzed by US-CERT, or information from federal partners.[23] This level of scrutiny is commonly referred to as "deep packet inspection."

Einstein "sensors" – computers equipped with government-configured software – perform this inspection by making a complete temporary copy of all network communications transmitted through a monitored section of the network while allowing the actual traffic to proceed unimpeded.[24] Einstein then scans the content of the copied communications, looking for matches with signatures of known cyber threats. If the communication does not include a signature of a known cyber threat, the copy is deleted.

If, however, the communication does contain a match to a threat signature, the *complete* communication is sent to US-CERT, where the information is saved on a separate network under US-CERT control. A US-CERT analyst may then examine the communication for further information related to the potential threat. The information saved and examined by US-CERT contains the substance of the communication which triggered the alert and may also include PII.[25]

---

line, which can contain content) using a court order . . . . Conversely, the interception of email contents, including the subject line, requires compliance with the strict dictates of Title III.).

[19] Such anomalies included configuration problems, unauthorized network traffic, network backdoors, routing anomalies, network scanning activities, and baseline traffic patterns. Einstein PIA 1, at 8.

[20] Einstein PIA 2, at 10.

[21] While Einstein 1 only captures flow record information, Einstein 2 captures and reviews significantly more data. Flow record data includes IP addresses but does not include any additional individual identifiers. Einstein 2 will observe and analyze all network traffic that connects to a federal executive agency IT system. *See* Einstein PIA 2, at 10.

[22] *Id*. at 3, 6.

[23] *Id.* at 3-4.

[24] *Id.* at 12-14.

[25] *Id*. at 5, 12-14.

1. Safeguards Within the Einstein 2 System

DHS asserts that safeguards are in place to reduce potential privacy threats posed by the Einstein 2 system. Network traffic not containing malicious activity signatures is never viewed by US-CERT personnel. Einstein 2's intrusion detection system generates a detailed log that records each command run on the system, so unauthorized use of the system can be detected and tracked.[26] The information that is captured may be stored by US-CERT for up to three years, but is deleted sooner if found to be unrelated to a threat.[27] US-CERT personnel who review the information are subject to oversight and receive annual training from the DHS Privacy Office.[28]

Even with these measures in place, US-CERT is presently able to disseminate information gathered by Einstein 2 internally or to other government agencies in an uncontrolled and unpredictable manner, without anonymization procedures in place.[29] US-CERT may share the raw network information collected through Einstein 2 with the specific agency on whose network the malicious activity was discovered.[30] US-CERT can also notify law enforcement, intelligence, and other agencies responsible for securing the federal network when a computer network event occurs that falls under their responsibility and provide them with the contact information at the affected participating federal agency to facilitate direct coordination.[31] Without proper safeguards in place, however, it is possible that a law enforcement agency may be able to gain access to the content of the communications from the affected agency, even though it would not have been able to gain such access directly from US-CERT.

C. EINSTEIN 3

In 2010, DHS released a Privacy Impact Assessment ("PIA") for a test run of the third version of Einstein.[32] Einstein 3's purpose is to detect and characterize malicious network traffic and respond appropriately to cyber threats by blocking the traffic before harm is done. This immediate response is termed "intrusion prevention." An Einstein 3 sensor will be installed at a private internet service provider ("ISP") to intercept traffic before it enters the federal network.

---

[26] Einstein PIA 2, at 12-14.
[27] *Id.*
[28] *Id.* However, the recent privacy compliance review of Einstein 2 and the field test of Einstein 3 reveal that although new staff and experienced staff receive basic DHS privacy training, they have not received privacy training specific to the Einstein program since November 2010. To correct this deficiency, the report recommends that position-specific privacy training be re-established for all staff. Einstein PCR at 7-8.
[29] In fact, although the sharing of information internationally was not directly mentioned in any of the Einstein PIAs, US-CERT collaborates with foreign governments and shares cyber threat reports. In its privacy compliance review, the DHS Privacy Office did not find any standard operating procedures outlining what information to share with, and what information to withhold from, foreign governments. It also reviewed two MOAs entered into with Israel and India and found that these agreements did not contain any restrictions or guidelines on sharing information such as PII. The DHS Privacy Office recommends that going forward US-CERT should include a provision regarding the sharing of PII in all MOAs with foreign partners. Einstein PCR at 7.
[30] *Id*. at 15.
[31] *Id.* at 16.
[32] Einstein PIA 3, at 1. The purpose of the Einstein "Initiative Three Exercise" was to demonstrate the ability of an existing ISP, designated as a Trusted Internet Connection Access Provider (a "TICAP"), to select and redirect internet traffic from a single participating government agency through an Einstein 3 sensor, which is essentially an Einstein 2 sensor modified with additional software from the National Security Agency ("NSA") that includes intrusion prevention technology.

A flagged communication will also be copied and stored for further analysis by US-CERT to determine its potential harm to the network. US-CERT will have access to the substance of the communication that triggered the alert, which may include PII of individuals involved in the communication or individuals whose computers were hijacked for an attack.[33]

Einstein 3 will also enable enhanced information sharing between US-CERT and federal agencies by giving DHS the ability to issue automated alerts of detected network intrusion attempts and, when necessary, to send alerts to the National Security Agency ("NSA").[34] The NSA will then assist DHS in using this information to "discover critical information about foreign cyber-threats and . . . inform Einstein 3 systems in real time."[35] During this assistance, it is possible that the content of communications will be reviewed by both DHS and NSA to develop a complete assessment of the potential threat. Although DHS has developed and published a PIA, NSA has not done so. Thus, there is a real risk that NSA may review communications from U.S. persons that have not been anonymized, and without any implementation by NSA of privacy safeguards.

1. Information Sharing Under Einstein 3

According to DHS, US-CERT may also disseminate collected information for non-cybersecurity purposes – including law enforcement and intelligence – "when the recipient is a federal, state, or local law enforcement entity and the information appears to indicate activities which may violate laws which the recipient is responsible to enforce or an agency of the federal government authorized to receive such information in the performance of a lawful government function."[36] DHS states that information sharing will be "conducted in accordance with the laws and oversight for activities related to homeland security … in order to protect the privacy and rights of U.S. citizens."[37] DHS clarifies that communications describing potential criminal activity will not be collected unless the traffic also happens to be associated with cyber threats.[38]

Nevertheless, because any communication which matches a "signature" is flagged and stored for possible review, there is real potential for erroneous capture and subsequent transfer of information. Signatures do not need to be complex computer code. To illustrate, viruses are often embedded in emails and, once those emails are opened, the viruses immediately spread to all of the recipients' email contacts. The signature for a virus could conceivably be simple text also found in innocent communications, thereby causing Einstein to tag both viral and innocent content. Similarly, if a hacker were to take over an individual's computer and use it to send malware without the owner's knowledge, the owner's legitimate communications could also be flagged as originating from that computer. Under both of these circumstances, Einstein could tag many communications for review by US-CERT even though the computer's owner violated no law. Thus, as discussed further below, we believe that it is important to impose meaningful use restrictions that limit the purposes for which government may use such shared data as well as the circumstances under which these data may be used.

---

[33] *Id.* at 7.
[34] *Id.* at 3.
[35] *Id.*
[36] *Id*. at 13-14.
[37] *Id.* at 3.
[38] *Id.* at 7.

III. REVIEWING THE OLC'S FOURTH AMENDMENT ANALYSIS OF EINSTEIN

A. EINSTEIN RAISES LEGITIMATE FOURTH AMENDMENT CONCERNS

The Fourth Amendment bars unreasonable searches and seizures of private property. In the absence of consent, where an individual has a reasonable expectation of privacy, the government must have probable cause and obtain a warrant authorizing a search. The capture, analysis, and sharing of communications by Einstein technology could potentially threaten our Fourth Amendment rights. These concerns are now heightened as Congress contemplates expanding Einstein technology and developing information sharing programs that allow government access to data from private industry networks.[39]

The OLC has advised DHS that the Einstein program, in its current form, does not violate the Fourth Amendment and, if expanded to monitor private networks, likely would not violate those constitutional rights. OLC's conclusion that expanding Einstein to monitor private networks would not violate the Fourth Amendment is questionable.

To determine whether DHS's capture and dissemination of PII withstands scrutiny under the Fourth Amendment, we reviewed the analysis upon which DHS currently relies to justify the Einstein projects. Between 2009 and 2010, the OLC issued two formal opinions addressing the legality of the Einstein.[40] Both opinions concluded that federal agencies can use Einstein to monitor government network traffic without infringing upon the Fourth Amendment rights of their employees or outside parties communicating with the agencies. To the extent that PII is collected and reviewed, OLC determined that agency network users have consented to government review of their emails, and therefore no warrant is necessary to review PII stored in the process of collecting communications matching the signatures of known cyber threats.

To clarify that users should not have any expectation of privacy, OLC advised federal agencies to implement a log-on banner or user agreement prompt that notifies agency network users that, in the interests of cybersecurity, network activity is subject to monitoring.[41] The purpose of these banners and agreements is to ensure that employees are aware of the Einstein program and consent to the monitoring process. Obviously, however, these banners and user agreements are not displayed to agency outsiders who communicate with government employees.

---

[39] *See, e.g.,* Fred H. Cate, *Comments to the White House 60-Day Cybersecurity Review*, Indiana University Center for Applied Cybersecurity Research 1 (March 27, 2009).

[40] *See* Memorandum for Fred F. Fielding, Counsel to the President, from Steven J. Bradbury, Principal Deputy Assistant Attorney General, Office of Legal Counsel, *Re: Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (EINSTEIN 2.0) to Protect Unclassified Computer Networks in the Executive Branch* (Jan. 9, 2009); *see also* Memorandum for Associate Deputy Attorney General, from David J. Barron, Acting Assistant Attorney General, *Re: Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch* (Aug. 14, 2009).

[41] A log-on banner or user agreement would appear each time an employee logged onto a monitored network. It is unclear whether the OLC would expect a user agreement to be approved by a network user each time the user accessed the network.

OLC's analysis, particularly with regard to federal agencies, has some merit, as federal employees arguably recognize the need to protect crucial federal networks when accepting their civil service positions. Expanding this argument to justify unregulated government access to communications across a host of private industry networks, however, is deeply concerning. Specifically, as discussed in Section III (B) and (C), below, we believe that Fourth Amendment rights are threatened if any government agency or organization outside of US-CERT reviews or disseminates the content of private communications accessed on private networks without first seeking judicial approval.

B. NETWORK COMMUNICATIONS ARE NOT FULLY PROTECTED BY THE FOURTH AMENDMENT

Although federal government employees will be aware that their network communications are monitored, non-employees (customers, vendors, family members, etc.) will not be aware of such government review. Therefore, non-employees may believe that they have a reasonable expectation of privacy with regard to communication flow records. However, the OLC argues that several federal court decisions indicate that there is no reasonable expectation of privacy in information contained in the to/from address fields in emails, IP addresses of visited websites, total traffic volume of the user, and any other addressing and routing information necessary to transmit communications over the internet.[42] Federal courts have concluded that establishing a network connection to transmit data through computer networks is equivalent to dialing an operator on a telephone and asking to connect to another person's phone.[43] There is no reasonable expectation of privacy concerning the fact of the transmission because one must willingly inform the network to send the data.[44] Thus, the government's capture of information contained in flow records identifying the source of suspect signatures is, as the OLC states, likely not considered a "search" under the Fourth Amendment.

Similar to telephone numbers or addresses written on envelopes that are provided to the telephone company or postal service in order to connect a telephone call or deliver mail, email and IP addresses provide routing information to ISPs to enable these service providers to deliver electronic communications. Telephone and postal service users have no reasonable expectation of privacy in the telephone numbers they dial and the addresses they write on envelopes. Although the extension of this analogy to flow records appears reasonable, we do not agree that

---

[42] *See Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 904-05 (9th Cir. 2008); *U.S. v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008); *see also Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) (no legitimate expectation of privacy in dialing, routing, addressing, and signaling information sent to telephone companies).

[43] "[W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company." *Smith v. Maryland*, 442 U.S. 735, 742 (1979); *U.S. v. Forrester*, 512 F.3d 500, 504 (9th Cir. 2007) ([Computer] surveillance is analogous to the use of a pen register that the Supreme Court held in *Smith v. Maryland*…did not constitute a search for Fourth Amendment purposes."

[44] We appreciate that the analogy to phone records may not be exact and constitutional rights are implicated to a greater extent in the email context. The Supreme Court has recognized that the right to free expression includes the right to do so anonymously, *see, e.g., McIntyre v. Ohio Elections Commission,* 514 U.S. 334, 343 (1995), and email addresses, which include domain names, may suggest political, religious, or other affiliations, and therefore be more revealing than phone numbers. However, we are less troubled by this risk in the email context than by the threat of unrestricted government access to content. For example, individuals could take steps to sign up for email addresses at domain names that do not suggest any such views or affiliations to secure their right to petition the government anonymously.

these same doctrines also justify review of the *content* of electronic communications. OLC extrapolates from its conclusion that US-CERT may obtain and review flow records without a warrant, and further concludes that all PII associated with flagged communications may also be captured, reviewed, and shared, without redacting information or seeking a warrant, under the banner of "cybersecurity."[45] OLC's conclusions in this regard are too far-reaching.

C. CONTENTS OF NETWORK COMMUNICATIONS ARE PROTECTED BY THE FOURTH AMENDMENT

Although private citizens have no reasonable expectation of privacy in the basic information contained in communication flow records, they do have a legitimate expectation of privacy in the content of their communications while they are in transit.[46] Disclosure of information necessary to transmit data across a network does not imply willing disclosure of the *content* of the transmitted communications. This is a distinction the Supreme Court has repeatedly identified as the boundary between consenting disclosure and unreasonable invasion of privacy.[47] The content of an email or other network communication is analogous to the contents in a sealed envelope;[48] those contents are not willingly disclosed to anyone but the recipient, and "the government cannot engage in a warrantless search of sealed mail."[49] As noted above, the subject line of an email, which is more revealing than basic to/from information, is generally considered to be part of the content.

However, the third-party doctrine provides a potential loophole for access to the content of communications when those communications are turned over to the government by a third party. According to a 1976 decision by the Supreme Court, individuals do not have a right of privacy with regard to information willingly turned over to a third party, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[50]

The OLC uses the third-party doctrine to justify the Einstein program's interception, copying, and monitoring of the content of communications between private individuals and

---

[45] OLC states that all PII capture should involve "minimization procedures" to mitigate privacy concerns. *See* January 9 OLC Memorandum, *supra* note 33, at 20. However, without any real description of what those procedures are, and given that the OLC asserts in the same memorandum that all communications are subject to legal review, we must assume all communications can be stored, read, and shared.

[46] Similar to the sender of a letter through the postal service, the sender of an email has a reasonable expectation of privacy in the content of the message while it is in transit. *See, e.g.*, *U.S. v. Lifshitz*, 369 F.3d 173, 190 (2d. Cir. 2004) (analogizing an individual's expectation of privacy when communicating through the postal service with an individual's expectation of privacy when communicating through email); *U.S. v. Maxwell*, 45 M.J. 406, 418 (C.A.A.F. 1996) (the sender of an email "enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant"); *see also Quon*, 529 F.3d at 905 ("[U]sers do have a reasonable expectation of privacy in the content of their text messages vis-à-vis the service provider.").

[47] *See Smith v. Maryland*, 442 U.S. at 735. *See also Forrester*, 500 F.3d at 511; *Quon v. Alexander, 529 F.3d 892 (9th Cir. 2008)*.

[48] *See Smith v. Maryland*, 442 U.S. at 735; *see also U.S. v. Maxwell*, 45 M.J. 406, 418 (C.A.A.F. 1996).

[49] *Forrester*, 500 F.3d at 511. This analogy applies to other communications as well. *See Quon*, 529 F.3d at 898 (stating text messages are equivalent to letters, telephone calls and email for the purposes of Fourth Amendment analysis.); *see also Smith v. Maryland*, 442 U.S. 735, 743 (1979).

[50] *U.S. v. Miller*, 425 U.S. 435, 443 (1976); *see also SEC v. Jerry T. O'Brien*, 467 U.S. 735 (1984); *U.S. v. Lifshitz*, 369 F.3d 173 (2d Cir. 2004).

federal employees transmitted over the federal network. The OLC extends this argument to cover communications to a federal employee's personal email account if that employee reads his personal email on a government computer, even if the private individual is unaware that the federal employee works for the government or that all of his communications, including personal ones, are monitored. The OLC argues that the sender of an email loses his reasonable expectation of privacy in the content of a message when the message is received; once the recipient receives an email, he has the right to disclose it to whomever he wants, whether it is to another private party or a government agent. Therefore, information passed between private individuals and federal agency employees ceases to be private when it reaches its recipient, even if that third-party recipient assured the sender of its confidentiality.[51] As a practical matter, this argument is not analogous to the process by which Einstein would store – and US-CERT would review – information captured off of private networks. Einstein identifies and copies communications while that data is *en route* through the network to a recipient (i.e., when the sender still has a reasonable expectation of privacy in the content of his communication).[52] Moreover, although courts may allow US-CERT to review information willfully disclosed by employees under certain circumstances, we are concerned that under this analysis individuals' privacy could be compromised because they are unaware that a recipient is a federal employee or that his private email accounts could be monitored.

We are also concerned that the third-party doctrine could be relied upon to permit government access to personal information stored and transmitted over purely private networks. This risk occurs if, as discussed below, Congress enacts legislation that would permit the federal government to scan critical private networks (e.g., banks, hospitals, and airlines) under its cybersecurity program, or even if – as appears more likely – there is no direct government monitoring but the legislation enables the private sector to share information with the government. We do not believe that the third-party doctrine should be extended to apply so broadly in the digital age. We do not agree that individuals can be said to have consented to government access to their personal information that they transmit over private networks. Scholars and courts have recently been reconsidering the reach of the third-party doctrine, and federal courts should not be willing to extend its application to permit government monitoring of or access to all communications on critical private networks.

Our Liberty and Security Committee has previously discussed how application of the third-party doctrine in the digital age has been called into question.[53] Technology has changed dramatically since the Supreme Court first considered the third-party doctrine. Individuals have no choice but to store information with a third party to participate in many basic aspects of modern life, such as banking online, communicating by phone or email, or using credit cards.[54]

---

[51] *See, e.g., U.S. v. Miller*, 425 U.S. 435, 443 (1976); *O'Brien*, 467 U.S. at 743; *Lifshitz*, 369 F.3d at 190; *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001; *see also U.S. v. Katz*, 389 U.S. 347 (1967) (electronic surveillance is subject to Fourth Amendment protections).

[52] This is a necessary function of Einstein 3 as, unlike Einstein 2, Einstein 3's objective is to prevent cyber-attacks as well as identify them. *See* Randal Vickers, *Privacy Impact Analysis for the Initiative Three Exercise*, Department of Homeland Security, at 3 (March 18, 2009).

[53] *See* Constitution Project's Liberty and Security Committee, *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age* at 13 (2010), available at: http://www.constitutionproject.org/pdf/DataMiningPublication.pdf

[54] Justice Brennan recognized this flaw of the third-party doctrine in his dissent in *Miller*. 425 U.S. at 451 (Brennan, J., dissenting) ("For all practical purposes, the disclosure by individuals or business firms of their financial affairs to

Many of our day-to-day activities necessarily involve sharing digital information with third parties; unwavering adherence to the third-party doctrine in its current form would render the Fourth Amendment's privacy protections ineffective against government attempts to gather electronic information.[55] Accordingly, some courts have recently sought to eliminate or heavily restrict the third-party doctrine, including the highest courts of several states,[56] multiple United States courts of appeal,[57] and even the Supreme Court.[58] Therefore, we conclude that this doctrine should not provide a justification for the federal government to monitor private communications over private networks without judicial oversight.

D. USER AGREEMENTS AND LOG-ON BANNERS DO NOT ALWAYS CONSTITUTE CONSENT UNDER THE FOURTH AMENDMENT

To circumvent the issue of whether individuals have a reasonable expectation of privacy, OLC strongly urges federal and private employers to implement user agreements or log-on banners that generally disclose the Einstein program's monitoring procedures. When an employee accepts a network's terms of use, the employee acknowledges that his network communication is subject to monitoring.[59] According to the OLC, this acceptance constitutes "consent" to turn over information to US-CERT.

For federal employees, the analysis that employees consent to having Einstein monitor communications is likely reasonable given the overwhelming importance of protecting key federal agency networks. It is likely that federal employees are aware of this concern when accepting employment. In the federal employment context, because the State and the employer are one and the same, it is difficult to imagine a scenario in which federal agencies could maintain adequate cybersecurity without monitoring communications transferred through their networks. In this regard, OLC's constitutional analysis appears reasonable. The reasonableness of consent in this context should not, however, be used as justification to ignore safeguards that would shield federal employees' PII from being shared, or worse, disseminated to law enforcement for reasons unrelated to cybersecurity and without probable cause.

While there is currently no plan in place to use log-on banners to address Fourth Amendment concerns in the context of monitoring *private* network communications, several

---

a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account.").

[55] *See* Daniel Solove*, Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 Fordham L. Rev. 747, 753 (2005) (discussing the overreaching implications of the third-party doctrine's original application).

[56] *See* Stephen E. Henderson, *Learning from All Fifty States: How to Apply The Fourth Amendment And Its State Analogs To Protect Third Party Information From Unreasonable Search*, 55 Cath. U. L. Rev. 373 (2006) (twelve states' highest courts have rejected the third-party doctrine under their state constitutions).

[57] *See, e.g., U.S. v. Warshak*, No. 08-3997, slip. op. at 23 (6th Cir. Dec. 14, 2010); *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892 (9th Cir. 2008), *rev'd on other grounds by City of Ontario v. Quon*, 130 S. Ct. 2619 (June 17, 2010).

[58] *Ferguson v. City of Charleston*, 532 U.S. 67, 83-84 (2001); *Georgia v. Randolph*, 547 U.S. 103 (2006). *See also, United States v. Jones,* 2012 U.S. LEXIS 1063 (Jan. 23, 2012) (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

[59] *See Lifshitz*, 369 F.3d at 190; *U.S. v. Heckenkamp*, 482 F.3d 1142 (9th Cir. 2007); *U.S. v. Angevine*, 281 F.3d 1130 (10th Cir. 2002); *U.S. v. Simons*, 206 F.3d 392 (4th Cir. 2000).

flaws would lie with that approach. First, an entity connected to a monitored network would not only need to provide notice to its employees, but also to anyone unaffiliated with the entity that nonetheless communicates with it, such as customers of a bank or power utility. Second, it is not clear whether a user agreement or log-on banner on a private network constitutes either legal consent or a waiver of an end user's expectation of privacy. Generally, consent is only valid under the Fourth Amendment when it is a "free and unconstrained choice, rather than a mere acquiescence in a show of authority."[60] Private employees required to "consent" to a user agreement arguably do not have the right to refuse to give consent, and "coercion may be found where one is given a choice between one's employment and one's constitutional rights."[61] Individuals who vitally need to communicate with an entity on a monitored network for any number of conceivable reasons may similarly feel compelled to consent.

Further, the stated purpose of obtaining such consent is to detect unlawful network intrusion and protect networks from cyber-attacks. The fact that an individual may have consented to the copying and automatic screening of his or her communications for malicious signatures does not necessarily mean that the individual has also consented to having that information stored for human review or transferred to federal or local law enforcement. Even if an employee's "consent" to have his or her computer activity monitored for cyber threats as a requisite for employment were sufficient to permit the monitoring of a private network for malicious activity, it is far from clear that such "consent" would or should include permission to provide the PII contained in such communications to law enforcement.[62] Thus, it is critical that cybersecurity programs also include use restrictions that limit the extent to which and purposes for which the government may use personal information after obtaining it.

E. THE SPECIAL NEEDS DOCTRINE SHOULD NOT EXEMPT US-CERT FROM OBTAINING A WARRANT TO REVIEW THE CONTENTS OF NETWORK COMMUNICATIONS

OLC's strongest argument for warrantless access to captured PII is the "special needs" doctrine. Under the special needs doctrine, an otherwise unreasonable search may be considered reasonable if the search "serves special government needs, beyond the normal need for law enforcement."[63] Courts "balance the individual's privacy expectations against the Government's

---

[60] *U.S. v. Garcia*, 56 F.3d 418, 422 (2d Cir. 1995) (internal quotation and citation omitted). The Committee does not hold the position that federal agencies are seeking to coerce their employees by expecting them to carefully consider their use of federal networks and equipment, as civil service inherently involves being held to a high standard. By contrast, however, private industry employment does not carry this additional expectation of serving the American people and, thus, private employees cannot be expected to subjugate their Fourth Amendment rights merely to gain employment.

[61] *Anobile v. Pelligrino*, 303 F.3d 107, 124 (2d Cir. 2001); *Garrity v. New Jersey*, 385 U.S. 493, 496 (1967). Although courts have upheld certain diminished employee rights under the Fourth Amendment, those cases often involve sensitive, government employee positions, such as a drug enforcement officers being subjected to invasive drug testing. *See, e.g., Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656 (1989).

[62] Nor can the government rely on the argument that a third party – in this case, the private industry authorizing Einstein oversight – has willingly turned this information over. Federal Courts have recently rejected this argument as well, distinguishing *U.S. v. Miller,* the authority relied on by OLC for such action, from the case at hand. *See U.S. v. Warshak*, No. 08-3997, slip. op. at 23 (6th Cir. Dec. 14, 2010) ("*Miller* is distinguishable [because] *Miller* involved simple business records, as opposed to the potentially unlimited variety of 'confidential communications' at issue here.").

[63] *Von Raab*, 489 U.S. at 665.

interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context."[64] For the same reasons that judicial scrutiny is applied to government wiretapping requests, judicial review is an appropriate safeguard that should be implemented regarding governmental monitoring of vast amounts of privately communicated data, particularly because the information may be used for traditional law enforcement purposes.

The government clearly has a vital interest in protecting our national cyber-infrastructure beyond the typical need for law enforcement.[65] OLC argues that this vital interest makes it impractical for government agencies outside US-CERT to obtain a warrant to review and share captured PII. Because Einstein 3's purpose is to detect and prevent a network attack, obtaining a warrant to review PII attached to flagged communications would be impractical only in situations in which it was necessary to review the PII immediately to prevent or terminate a cyber-attack. In other circumstances, a government agency should demonstrate probable cause to obtain a warrant swiftly or, instead, review the communications in "redacted" form that only reveals flow records and the targeted threat signature.

In most cases there would be no "special need" for US-CERT to share such PII with other law enforcement branches seeking review without a warrant, or even to share the information internally beyond the initial review. Since the asserted special need is to detect and eliminate network attacks, it would not be necessary to share PII with traditional law enforcement beyond a targeted threat signature or flow record. Although the special needs doctrine "does not require employing the least intrusive means," those means "must bear a close and substantial relation" to the government's interest in pursuing the search.[66] If US-CERT wants to capture and monitor communications containing targeted threat signatures to prevent cyber-attacks, reviewing PII beyond the signatures and flow records hardly "bears a close and substantial relation" to that goal. If DHS wants to identify and apprehend a perpetrator, then the threat signature's existence alone makes obtaining a warrant far from impractical.

Because the government would essentially monitor all communications sent across vital networks, there is a risk that its actions would be akin to a mass wiretapping program. The Wiretap Act and the Foreign Intelligence Surveillance Act ("FISA") statutes, among others, prohibit the government from engaging in domestic electronic surveillance without a court order. Although there are important exceptions to these court order requirements, such as for cases of exigent circumstances, federal officials are not permitted to indiscriminately monitor Americans' electronic communications.[67] Although we do not mean to suggest that cybersecurity programs would literally violate the terms of these statutes, monitoring American's private email communications and internet traffic could resemble "electronic surveillance," which is defined

---

[64] *Id.* at 665-66.
[65] *See* Cate, *Comments to the White House 60-Day Cybersecurity Review*, at 2 ("information in the private sector is critical to protect valuable data and communications systems, to secure systems that control other elements of critical infrastructure . . . and to secure other . . . networks that connect with those private-sector systems.").
[66] *U.S. v. Lifshitz*, 369 F.3d 173, 192 (2d Cir. 2004) (citing *Bd. if Educ. v. Earls*, 536 U.S. 822, 837 (2002).
[67] *See* 18 U.S.C. §2511(1); 18 U.S.C. §2516(1) (authorizing electronic surveillance subject to a judicially authorized wiretap order for generally no longer than 30 days); 18 U.S.C. §§2516-18 (imposing detailed requirements to obtain a wiretap order); 50 U.S.C. §1809 (prohibiting domestic wiretapping of U.S. citizens under the Foreign Intelligence Surveillance Act).

for the purposes of foreign intelligence surveillance as the "use of an electronic, mechanical or other surveillance device in the United States for monitoring to acquire information . . . under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes."[68] Further, the Wiretap Act covers not only telephone communications, but also electronic programs that automatically read internet traffic.[69]

Thus, even when the government's "special needs" justify sharing PII with the NSA or other federal agencies to prevent an attack on national security, the absence of a warrant or similar authority may be unreasonable. NSA's function in coordinating with US-CERT is to determine if a potential network attack is the effort of foreign national operatives. The concern with requiring the NSA to obtain a warrant is the possible public exposure of confidential national security information and activity. Without question, national security is of the utmost importance, and protecting critical classified information is a key element of that objective.

To prevent this type of conflict in the context of foreign intelligence surveillance, FISA established the Foreign Intelligence Surveillance Court ("FISC") to allow the judiciary to review such requests for information and still maintain the confidence of national secrets.[70] FISA statutes already provide specific rules for obtaining approval to monitor an individual's communications. Similar rules should be applied to government cybersecurity technology so that the protection of critical infrastructure does not threaten civil liberties.

Even under extreme or otherwise justified circumstances, an infrastructure is in place to authorize government searches of private information while protecting the rights established under the Fourth Amendment. It is imperative that this proven system of checks and balances remains an indispensable part of national security as the government seeks to expand cybersecurity initiatives into the private sector.

IV. THE EXISTING CYBERSECURITY LEGAL FRAMEWORK

Expansion of the Einstein program into the private sector would materially impact the existing legal framework under which government cybersecurity currently operates. As Congress itself has pointed out, nearly fifty laws already exist that serve as the legal infrastructure for allowing the government to monitor federal networks and their communications.[71]

For example, the Counterfeit Access Device and Computer Fraud Abuse Act of 1984 prohibits attacks on federal computer systems and on those used by banks in interstate

---

[68] 50 U.S.C. §1801(f)(4).

[69] The Electronic Communications Privacy Act amended the Wiretap Act to include electronic communications. 18 U.S.C. §2510-2521; *see also* Samantha L. Martin, *Interpreting the Wiretap Act: Applying Ordinary Rules of "Transit" to the Internet Context*, 28 Cardozo L. Rev. 441 (2007).

[70] The FISC courts were created specifically to oversee requests for warrants by federal agencies to monitor and review private communications, in a manner that is secret to the public and does not publicize any evidence disclosed during judicial proceedings. *See, e.g., In re Sealed Case*, 2002 Extra LEXIS 576 (F.I.S.C.R. 2002).

[71] Fischer, Eric A., *Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions*, Cong. Research Serv. 1 (Dec. 7, 2011).

commerce.[72] However, the Electronic Communications Privacy Act prohibits eavesdropping on U.S. citizens, such that the government cannot secretly monitor individuals suspected of a possible attack without express judicial authority.[73] The Computer Security Act of 1987 authorized the National Institute of Standards and Technology ("NIST") to develop cybersecurity standards for federal agencies, and the Federal Information Security Management Act of 2002 strengthened those responsibilities and authorized the Office of Management and Budget to effect those standards.[74] While the Homeland Security Act of 2002 granted added authority to DHS to monitor critical government networks,[75] existing laws restrained DHS from infringing on civil liberties as this task was undertaken. These are just a few laws that constitute the existing legal framework. In order for Congress to advance cybersecurity and meaningfully protect critical network infrastructure while protecting individuals' right to privacy, the existing legal framework must be reviewed and holistically updated.

V. CONGRESSIONAL CYBERSECURITY INITIATIVES

Various members of Congress have introduced legislation in recent years that would codify the Einstein program, as well as develop other cybersecurity initiatives, to provide the executive branch with clear legislative authority to oversee cybersecurity within the federal government and across critical private sectors.[76] Members of the 112th Congress have taken up that torch and introduced S. 21, a "Sense of Congress" highlighting its intent to pass comprehensive cybersecurity legislation in 2011.[77] Two bills from the 111th Congress (one already reintroduced in the 112th Congress), a report issued by the House Republican Cybersecurity Task Force, and two bills recently introduced in the House provide a general framework for Congress' legislative goals in the coming year.[78]

---

[72] 18 U.S.C. § 1001 et seq. (1984). As subsequent court decisions have noted, abusers need only intended to illegally access a federal system, whether the system is ultimately damaged or not. *See U.S. v. Morris*, 928 F.2d 504 (2d Cir. 1991).

[73] 18 U.S.C. § 2510-2522 (1986).

[74] The 2002 law effectively revised and repealed the 1987 legislation in order to clarify the roles of government agencies in the context of cybersecurity. 44 U.S.C. § 3541 et seq. (2002).

[75] Pub. L. No. 107-296, 116 Stat. 745 (Nov. 25, 2002). As already noted, the DHS mandate was updated through President Bush's 2008 Comprehensive National Cybersecurity Initiative. *See supra*, Section I.A.

[76] The need to codify the Einstein program is heavily rooted in the statutory provisions of the Foreign Intelligence Surveillance Act. It is legally questionable under FISA whether Einstein can be used to perform its "surveillance" for more than 48 hours without a warrant or some additional statutory authority. Legislation codifying the Einstein program would help resolve this issue. *See* Foreign Intelligence Surveillance Act, 50 U.S.C. § 1809 (2008).

[77] *See* Cybersecurity and American Cyber Competitiveness Act of 2011, S. 21, 112th Cong. (2011). In a November 2011 letter, Senator Harry Reid (D-Nev.) wrote to Senator Mitch McConnell (R-Ky.) that he would "bring comprehensive cyber security legislation to the Senate floor for consideration during the first Senate work period of next year." Letter from Harry Reid (D-Nev.), Senate Majority Leader, to Mitch McConnell (R-Ky.), Senate Minority Leader (Nov. 16, 2011) (available at http://www.securityprivacyandthelaw.com/uploads/file/Reid%20letter[1](1).pdf).

[78] Senate Majority Leader Reid recently stated, along with the introduction of S. 21, that whatever cybersecurity legislation is eventually passed will be an amalgamation of various bills dissected by several House and Senate committees covering commerce, science and technology, armed services, intelligence, foreign relations and energy. *See* Privacy Security Law Report, "Reid, Committee Chairs Urge Enactment of Comprehensive Cybersecurity Measure, http://news.bna.com/pvln/PVLNWB/split_display.adp?fedfid=19152010&vname=pvlrnotallissues&fn=19152010&jd=a0c6e6e8k8&split=0 (Jan. 31, 2011).

A. S. 413: THE CYBERSECURITY AND INTERNET FREEDOM ACT OF 2011

Senator Joseph Lieberman introduced S. 413, the Cybersecurity and Internet Freedom Act of 2011, an updated version of S. 3480 from the 111th Congress. The fundamental purpose of S. 413 is to "modernize the federal government's ability to safeguard the nation from cyber attacks."[79] S. 413 covers a vast number of initiatives to help the federal government better manage cybersecurity in the long term, including expanding budget outlays and developing risk management strategies. S. 413 would enable the private sector to develop cybersecurity technologies without the risk of exposing cyber networks to vulnerabilities. S. 413 addresses the government role in cybersecurity through a few key provisions.

First, S. 413 would authorize an Office of Cyberspace Policy within the Executive Office of the President, tasked with developing a national strategy that would guide cybersecurity efforts across intelligence, military, diplomatic, law enforcement, and commercial agencies within the federal government, and ensure that cybersecurity procedures and other vital information are shared fully across federal agencies. The Director of Cyberspace Policy would be granted access to classified and unclassified military, intelligence, and law enforcement information that is relevant to protecting the national cyber infrastructure.

S. 413 would also establish the National Center for Cybersecurity and Communications ("NCCC") within DHS. The NCCC's primary charge would be to lead the federal effort to secure and protect the federal information infrastructure as well as critical private network infrastructures. In doing so, the NCCC would absorb US-CERT, and with it the Einstein program. It would coordinate with both federal agencies and the private sector to develop and approve best practice policies, share critical information, and oversee the execution of cybersecurity strategies. The NCCC would also be authorized to disclose classified or confidential information relevant to cybersecurity threats and vulnerabilities to the owners and operators of certain private sector networks, whenever necessary to protect them from both foreign and domestic cyber-attacks. Such disclosure would potentially create situations in which private employees' personal communications are passed on to employers as well as various federal law enforcement agencies.

S. 413 would also authorize the president to declare a national emergency to critical national network infrastructures, both federal and private, allowing the president in undefined ways to take control of protecting those infrastructures. The president would be required to notify Congress, as well as owners and operators of critical private networks, before doing so. Unlike its predecessor bill in the 111th Congress, S. 413 does contain a few limitations on the use of this new emergency power, such as clarifying that emergency orders remain in effect only up to 30 days, and are renewable up to 120 days before Congressional authorization is needed to continue exercising the emergency authority. The bill also states that the government shall not "control covered critical infrastructure," and that it can interfere or prohibit communications only when 'no other emergency measure or action' will preserve the operability of the communications system.[80] These are substantial and important limitations on the use of what has

[79] *See* S. Rep. No. 111-368, at 1 (2011) (Senate Report for S. 3480, the legislative predecessor to S. 413).
[80] S. 413, The Cybersecurity and Internet Freedom Act, 112th Cong. (2011), §249(a)(6) .

been coined a "kill switch," but the bill explicitly reserves the right of the executive branch to invoke such a power.

Significantly, S. 413 does not expand the government's authority to collect cybersecurity information. Rather, it clarifies that current criminal and foreign intelligence wiretapping laws do apply. S. 413 directs private entities to share incident information with the NCCC, but requires such information sharing conform with privacy laws already on the books.

For these key initiatives, S. 413 also mandates the Director of the NCCC, in conjunction with a "privacy officer" within the NCCC, to develop oversight policies. These policies must ensure that all information monitored, collected, and shared for the purposes of cybersecurity is adequately protected, and that those protections are routinely monitored to ensure compliance among all agencies and critical private network operators. Although the language of S. 413 is somewhat vague, particularly with regard to who would be responsible for this oversight and how, the NCCC is required to comply with NIST and Federal Information Security Task Force policies for protecting information, including PII.[81] The OMB is required to submit a report assessing the quality of these safeguards within one year of enactment of the legislation.

B. S.773: THE CYBERSECURITY ACT OF 2010

Senator Jay Rockefeller (D-W.Va.) introduced S. 773, the Cybersecurity Act of 2010, in the 111th Congress and has stated his intent to reintroduce the bill in the current session.[82] S. 773 seeks to "strengthen the security of the American information infrastructure by expanding the information security workforce, establishing authorities for the Federal government, and enhancing public-private collaboration."[83] It is similar in many regards to S. 413.

Like S. 413, S. 773 requires the president to identify private network infrastructures that are critical to national cybersecurity, and authorizes the president to take control of those networks during an emergency. Unlike S. 413, however, the Rockefeller bill (S. 773) does not address the "kill switch" issue. S. 773 would also *require* owners and operators of critical private networks to adhere to whatever best practices are determined by a new, centralized cybersecurity agency. The cybersecurity agency would collaborate with the private sector and would grant private network owners and operators access to information, possibly classified or confidential, that is deemed vital to protecting private sector networks from identified threats and vulnerabilities.

S. 773 would direct the comptroller general to review federal laws applicable to cybersecurity to ensure that personal privacy and civil liberties, particularly those addressed under the Privacy Protection Act and the Electronic Communications Privacy Act, are protected. S. 773 demands that Executive cybersecurity officials set forth requirements for promulgating information sharing rules and procedures that ensure confidentiality and privacy protections for

---

[81] *See, e.g.*, Office of Mgmt. & Budget, Exec. Office of the President, OMB Memorandum No. M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007).
[82] Additionally, Representative Bennie Thompson (D – Miss.) has introduced legislation similar to S. 773 in the House Committee on Homeland Security. *See* Homeland Security Cyber & Physical Infrastructure Protection Act of 2011, H.R. 174, 112th Congress (2011).
[83] S. Rep. No. 111-384, at 1 (2010).

PII, and for private-sector owned intellectual property and proprietary information. S. 773 would also create a Cybersecurity Advisory Panel to represent law enforcement as well as civil liberty concerns in advising the president.

S. 773, although similar in scope, is notably more vague than S. 413 regarding integrating US-CERT operations into the ultimate agency responsible for overseeing national cybersecurity policy. S. 773 also focuses much more on expanding budget outlays for job creation related to cybersecurity and research grants for developing cybersecurity technologies.

C. HOUSE CYBERSECURITY INITIATIVES

On October 5, 2011, the House Republican Cybersecurity Task Force issued its recommendations for cybersecurity legislation.[84] The task force concluded that any legislation enacted should be targeted and limited and that private sector cooperation should be encouraged through the use of voluntary incentives. Noting that information sharing among industries and between government and industry is essential to improve cybersecurity and to prevent cyber-attacks, the task force recommended the creation of a new entity to facilitate this information sharing. The entity would be separate from – but partially funded by – the federal government, thus limiting direct government monitoring of private networks. In addition to recognizing the need to limit government involvement with private networks, the report states that any information shared with the federal government should have "sensitive personally identifiable information from Americans removed and sanitized" before it is shared.[85] We agree that the sanitization and anonymization of Americans' PII is an essential part of any proposed cybersecurity initiative.

Unfortunately, H.R. 3523, The Cyber Intelligence Sharing and Protection Act of 2011, does not include a provision protecting Americans' PII. On November 30, 2011, Representative Mike Rogers (R-MI) introduced H.R. 3523. This bill poses a significant threat to Americans' privacy. H.R. 3523 would allow private companies to share its customers' private and personal information with the federal government for cybersecurity purposes without requiring those companies to sanitize or anonymize PII. At a minimum, the bill should be amended to (1) require the anonymization of customer PII before it shared with the federal government and (2) place explicit use restrictions on the federal government for any data shared between the federal government and private industry to ensure that it is not used for other purposes.

The House's most recently proposed legislation is H.R. 3674, the Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act (PrECISE). Although this bill would also promote and authorize information sharing between the government and the private sector, it also contains some provisions designed to protect Americans' PII. Introduced on December 15, 2011 by Representative Dan Lungren (R-CA) and eight other members, H.R. 3674 creates the National Information Sharing Organization ("NISO"), a private not-for-profit organization to facilitate information sharing between the government and the private sector. Modeled after the entity proposed by the House Republican Cybersecurity Task Force, NISO's

[84] House Republican Cybersecurity Task Force, *Recommendations of the House Republican Cybersecurity Task Force*, 112th Cong. (2011).
[85] *Id.* at 11.

board of directors would be composed of five representatives from the federal government, ten representatives from critical infrastructure owners and operators, two privacy and civil liberties experts, and the chair of the National Council of Information Sharing and Analysis Centers. H.R. 3674 instructs this board to develop a charter for NISO that addresses, among other things, (1) rules for sharing information among the private sector and between the federal government and the private sector and (2) protections of privacy and civil liberties. H.R. 3674 states that while NISO shall facilitate information sharing, it must also ensure that the information exchanged "shall be stripped of all information identifying the submitter and of any unnecessary personally identifiable information."[86]

D. EXPANSION INTO THE PRIVATE SECTOR

In sum, S. 413, S. 773, the House Republican cybersecurity task force recommendations, H.R. 3523, and H.R. 3674 amend and codify current cybersecurity initiatives such as the Einstein program that regulate government networks, clarify federal responsibility for cybersecurity programs, regulate the private sector's affirmative cybersecurity responsibilities, encourage information sharing between government and private networks, and in some cases grant emergency authorities.

In particular, all of the Congressional proposals promote information sharing and partnerships between the federal government and the private sector. This is an important and necessary strategy for combating the risk of cyber-attacks and other cyber threats. However, without robust safeguards, information sharing poses serious risks to individuals' privacy rights and civil liberties. The exact nature and extent of these risks will depend in large part on who will monitor private networks – the government or the private sector entities that operate private networks – as well as on the extent to which private companies share individuals' private information with the government. If the government itself monitors private cyber networks, the risks to privacy rights and civil liberties will expand dramatically. Similarly, if the private sector monitors and shares information with the government, it is important that programs incorporate robust protections for individual rights.[87]

If private sector actors routinely share electronic communications with the government, then government officials must apply the same privacy safeguards to these data as would apply if they had intercepted the communications themselves. This should include strict use restrictions that limit the extent to which and circumstances under which the government may use PII that it obtains. Similarly, government agencies must limit sharing PII and communication content with

---

[86] Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act (PrECISE), H.R. 3674, 112th Cong. § 242(1)(A) (2011).

[87] After final review of this report by Committee members, DHS issued *Privacy Impact Assessment for the National Cyber Security Division Joint Cybersecurity Services Pilot (JCSP) DHS/NPPD-021* on January 13, 2012. This report contains a discussion of privacy issues resulting from an information sharing pilot program between the federal government and Defense Industrial Base (DIB) companies in private industry. Although the report discusses the protection of PII and use restrictions, it does not consider the full scope of privacy issues that are raised by current legislative proposals that would affect the general American public – such as the sharing of content and customer PII – if such a program were extended to cover the entire private sector. *See Privacy Impact Assessment for the National Cyber Security Division Joint Cybersecurity Services Pilot (JCSP) DHS/NPPD-021* (2012) available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_nppd_jcsp_pia.pdf.

private sector actors. Safeguards should be incorporated both to protect individuals' privacy rights and to minimize the risk of inadvertent disclosures of sensitive personal information.

Many of the safeguards recommended in the particular bills described above, however, lack the specificity to ensure that the Fourth Amendment rights of individuals are not impacted as federal monitoring expands into private networks. Safeguards are also needed to limit the extent to which private data are transmitted to the government, and to protect the data that are shared.

VI. THE WHITE HOUSE CYBERSECURITY LEGISLATIVE PROPOSAL

S. 413, S. 773, H.R. 3523, and H.R. 3674 are just four of more than fifty cybersecurity bills introduced in recent sessions of Congress.[88] To help narrow the scope of these bills, Congress asked the White House to offer guidance on its goals for national cybersecurity. The White House obliged by submitting to Congress on May 12, 2011 a legislative proposal to overhaul federal cybersecurity laws.[89] The White House cybersecurity legislative proposal states that it seeks to update existing laws involving the protection of information, identify and safeguard the private network infrastructures that are critical to our national security, and ensure that the rights of individuals are not diminished as the federal government seeks to protect the health, safety, and economic security of America. Although the White House proposal relies heavily on future rulemaking to provide clearer definition to these new and updated policies, the proposal could impact individuals' privacy and civil liberties.

The White House proposal would create a federal law requiring customer notification any time a private network's security is breached that could result in the exposure of those individuals' sensitive PII. The proposal would also require DHS to develop and oversee the implementation of updated information system management policies across federal agencies to consistently manage and protect our government's highly networked infrastructure. These are important and helpful changes to the federal government's efforts to develop a comprehensive national cybersecurity system.

The White House proposal recommends that Congress enact the Department of Homeland Security Authority and Information Sharing Act. Similar to S. 413 and S. 773, this act would create a centralized national cybersecurity department that would not only monitor and protect federal agency systems, but help protect critical private networks as well.[90] The Act would direct the Secretary of DHS to issue rules that implement risk-based approaches to improve cybersecurity. As part of that process, DHS could share information with the private sector, non-federal governments, and other stakeholders to prevent cyber-attacks through a newly formed Cyber Security Center.

---

[88] *FACT SHEET: Cybersecurity Legislative Proposal*, The White House Office of the Press Secretary (May 12, 2011), http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal.
[89] *See* White House Cybersecurity Legislative Proposal Section-by-Section Analysis (May 12, 2011), http://democrats.senate.gov/pdfs/WH-cyber-section-by-section.pdf.
[90] White House Proposed Legislative Language, at 1 (May 12, 2011) http://democrats.senate.gov/pdfs/WH-cyber-general-authorities.pdf.

Under the Act, the Center would also protect federal systems by using an intrusion detection and prevention system—essentially codifying Einstein.[91] Like S. 413 and S. 773, the proposal calls for a rulemaking process to determine to what extent the intrusion detection system would operate, and the best practices to be used in collecting and sharing the information obtained through the system. Although the White House proposal does not explicitly authorize expanding Einstein into the private sector, Section 243 of the Act authorizes implementing cybersecurity technologies that will protect critical private information infrastructures, including technologies that provide incident detection, analysis, and mitigation.[92] We are concerned that this language could be read to authorize private expansion in the future if DHS, during the rulemaking process and in collaboration with government and private stakeholders, were to deem this necessary.

Further, Section 245 of the Act would explicitly authorize private entities that already intercept, acquire, or otherwise obtain network communications lawfully to disclose that information to DHS for the purpose of protecting information systems from cybersecurity threats, including sensitive PII or the contents of communications.[93] Under this section, DHS would share information garnered from monitored communications with other government agencies, including law enforcement if the information obtained is evidence of a crime, with the approval of the Attorney General.[94] The proposed language is not limited to cybersecurity crimes, meaning that any communication garnered in the interests of cybersecurity which ultimately implicated an individual in a non-cyber crime could be turned over to traditional law enforcement authorities. Depending on the level of influence asserted by the federal government on critical private industries, we are concerned that this language could authorize a virtual "wiretap" on critical private network communications under the banner of cybersecurity. This concern is particularly serious if DHS decides to expand Einstein to protect critical private infrastructures.

To assuage the clear concerns these policies would raise, Section 248 of the Act would require that such monitoring take place in accordance with policies designed to protect the privacy and civil liberties of individuals communicating across these networks.[95] Section 248 would direct the Secretary of DHS to develop and periodically review these protective policies, with the approval of the Attorney General and in consultation with privacy and civil liberty experts. Under the proposed bill, these policies should be written to minimize the intrusion detection system's impact on privacy and civil liberties; to limit the acquisition, storage and use of PII; to safeguard stored information; and to protect individuals' confidentiality.[96] Section 248 would also require the Chief Privacy and Civil Liberties Officer of the Department of Justice, in consultation with senior civil liberty officers from federal agencies, to submit a joint annual report to Congress assessing the privacy and civil liberty impact of the federal government's

[91] *Id*. at 5 ("Sec. 244. National Cybersecurity Protection Program"). The proposed language does not name Einstein specifically, but Einstein is currently the federal government's only intrusion detection and prevention system.
[92] *Id*. at 4 ("Sec. 243. Authority and Responsibility to Conduct Cybersecurity Activities").
[93] White House Proposed Legislative Language, at 7-8 (May 12, 2011) http://democrats.senate.gov/pdfs/WH-cyber-general-authorities.pdf.
[94] *Id*. at 8.
[95] *Id*.
[96] *Id*. at 9.

cybersecurity activities related to monitoring network communications.[97] Although these intended safeguards are laudable, they are general in nature and do not specifically address how violations of individuals' Fourth Amendment rights will be avoided or minimized. It is also unclear how these policies can be effective when other sections of the Act would authorize the use of information obtained by monitoring network communications to pursue traditional law enforcement means. Nor does the Act's language clarify how PII would be sheltered from government officials or private network operators reviewing private communications.

Finally, we note that the White House's proposed bill assigns to the Privacy and Civil Liberties Oversight Board (PCLOB) the responsibility to assess the privacy and civil liberties impact of the new cybersecurity program and report to Congress within two years after the legislation is enacted. Although we agree that the PCLOB would be an appropriate entity to conduct such oversight, as we have previously lamented, to date this Board does not exist.[98] It took from 2007, when Congress enacted legislation to revamp the Board and grant it greater authority and independence, until December 2011, before any president nominated a full slate of five members to serve on the Board. As of the date of this report, none of the five nominees have been confirmed by the Senate. We urge the Senate to act quickly on all five nominations so that the Board may finally begin its important work. We also recommend that beyond the PCLOB, any cybersecurity legislation should require periodic Inspector General audits and comprehensive reporting to Congress.

The White House's legislative proposal recognizes the important balance between securing our modern infrastructure and protecting the private content that Americans need to transmit electronically in this day and age. It is encouraging to know privacy and civil liberties have not taken a back seat as the executive branch has worked diligently to provide meaningful guidance to Congress. Many questions do remain, however, particularly with regard to how these safeguards would be implemented and whether they can provide real protection given the unavoidably intrusive nature of monitoring critical federal and private networks.

VII. RECOMMENDATIONS FOR THE IMPLEMENTATION OF SAFEGUARDS IN ANY COMPREHENSIVE CYBERSECURITY POLICY

For the reasons set forth in this report, we recommend the following reforms through forthcoming federal legislation or agency regulation:

ESTABLISH EFFECTIVE OVERSIGHT

1. Both Congress and the executive branch should work to clarify the nature and magnitude of the cybersecurity threat to the public so that the development and approval of comprehensive cybersecurity policies and public-private collaboration efforts are adequately shaped by the specific risks facing America's critical network infrastructure.

2. Any federal agency developing new or expanded cybersecurity programs should develop a Privacy Impact Assessment (PIA), even if one is not required by the E-Government

[97] *Id*. at 10.
[98] *See* The Constitution Project, *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age*, 22 (2010).

Act, to provide transparency for the program's development and ensure that personal privacy and civil liberties are being considered and protected.

3. Both legislation passed by Congress and subsequent federal regulations should include key metrics based on existing federal privacy laws such that the repercussions of extending the national cybersecurity initiative into the private sector can be reviewed and changed in the interests of protecting American citizens' right to privacy. The OMB and the agencies responsible for setting these metrics should conduct regular audits to review these metrics and their application on a recurring basis. In addition, federal agencies responsible for conducting cybersecurity programs should report regularly to Congress on these metrics.

4. As Congress clarifies and centralizes national cybersecurity authority, independent oversight should be established to ensure that constitutional safeguards are implemented and followed across federal agencies and private industry. The first step in this process should be fully establishing the PCLOB and filling all five of the Board's seats.

5. Legislation should require periodic mandatory audits by the inspectors general (IG) of the relevant agencies and should require that the IG reports include a discussion of the nature and amount of information being shared with the federal government and how it is used. These reports should be submitted to all congressional committees of jurisdiction and each IG should also prepare an unclassified version that will be made available to the public.

6. Congress should work closely with, and seek input from, DHS and other federal agencies so that duplicative and overlapping infrastructures are eliminated as legislation to centralize federal cybersecurity responsibilities is crafted. This meaningful step will ensure clear and effective communication between public and private participants so that cybersecurity efforts are fluid and successful and best practices for privacy safeguards are being shared and properly followed.

IMPLEMENT EFFECTIVE PRIVACY SAFEGUARDS

7. Congress and the executive branch should develop programs that rely, to the greatest extent possible, on private monitoring of private networks to achieve cybersecurity. As federal agencies work with the private sector to determine which "best practices" should provide the framework for information sharing, network risk management, and other cybersecurity policy, all parties should carefully consider the impact on civil liberties. These groups should provide a forum for individuals to express their privacy concerns and these concerns should be included as part of the best practices that will be followed by government and private agencies alike.

8. All cybersecurity programs relying on partnerships between the government and the private sector should include specific procedures to limit the sharing of PII between private sector and government actors. As recommended by the House Republican Cybersecurity Task Force, the procedures should require that data shared between the

government and the private sector should have "sensitive personally identifiable information from Americans removed and sanitized."

9. Any cybersecurity legislation, regulation, or agency directive regarding information sharing should require (1) strict time limits for data retention, (2) data anonymization whenever possible, and (3) policies to diminish the risk of inadvertent or improper disclosure when a cybersecurity program requires the collection and storage of information containing PII. PII should only be collected, retained or disseminated when it is necessary to protect against or mitigate a cybersecurity threat.

10. Congress and federal agencies should explicitly bar any private industries that are granted access to Einstein and other cybersecurity technology from individually storing or reviewing private communications for any purpose beyond the services required by the Einstein program.

11. Congress and federal agencies should implement safeguards that place meaningful restrictions on aggregating and/or sharing information obtained in the course of cybersecurity. PII should not be shared with law enforcement officials or relied upon as evidence of a non-cyber crime, unless the PII was legitimately obtained as a necessary component of the data specifically flagged as a possible cybersecurity threat. All other data included in flagged communications should be unavailable for review by traditional law enforcement without first obtaining a warrant.

12. Congress should conduct hearings in connection with proposed cybersecurity legislation, to consider carefully the privacy policies that will be undertaken by any new agency created to manage centrally US-CERT and the national cybersecurity initiative. Particularly, these hearings should evaluate how such policies relate to reviewing, redacting, and sharing potentially sensitive PII. These hearings should be opened to interested parties and field experts to provide perspective on civil liberty concerns and the extent to which government intrusion is necessary to effectively protect cyberspace. Congress should seek to ensure that any regulations mandating new policies are specific and clear, and that all agency policies are easily available so the public can provide valuable input on these measures as they are implemented.

LIMIT THE SCOPE OF ACCESS TO OR USE OF CONTENT

13. Congress should ensure that any and all new legislation and regulations regarding network monitoring and reviewing communication content include a definition of "content" as it is defined under the Wiretap Act.

14. Cybersecurity initiatives and technologies that involve the interception of wire, oral or electronic communications must comply with the Wiretap Act and other statutes governing electronic surveillance by government agencies, so that government officials seeking to obtain the content of such communications must first obtain a warrant or order from an appropriate court. All existing exceptions to these statutory requirements, such as the exception for exigent circumstances that would necessitate immediate action would continue to apply.

15. Cybersecurity initiatives and technologies intended to protect against threats from foreign powers and agents of foreign powers, including international terrorists, must comply with the FISA, so that where applicable, government officials seeking to obtain the contents of electronic communications must first obtain a warrant through the FISC. All existing FISA exceptions, such as for exigent circumstances, would continue to apply.

16. Congress should require that if federal agencies acquire content through cybersecurity operations, that information may only be used as necessary to implement the cybersecurity program and protect networks. Content should not be shared with law enforcement officials or relied upon as evidence of a non-cyber crime, unless the content was legitimately obtained as a necessary component of the data specifically flagged as a possible cybersecurity threat. All other data included in flagged communications should be unavailable for review by traditional law enforcement without first obtaining a warrant.

17. Congress should ensure that any and all regulations and policies emanating from the cybersecurity debate are written and implemented in a manner that prohibits or otherwise avoids cybersecurity operations that would result in favoritism or discrimination for political or other purposes.

MEMBERS OF THE CONSTITUTION PROJECT'S LIBERTY AND SECURITY COMMITTEE
Endorsing the Report on Cybersecurity*

CO-CHAIRS:

David Cole, Professor of Law, Georgetown University Law Center

David Keene, former Chairman, American Conservative Union

MEMBERS:

Bob Barr, former Member of Congress (R-Ga.); CEO, Liberty Strategies, LLC; the 21st Century Liberties Chair for Freedom and Privacy, the American Conservative Union; Chairman, Patriots to Restore Checks and Balances; practicing attorney in Atlanta, GA

Phillip J. Cooper, Professor, Mark O. Hatfield School of Government, Portland State University

John W. Dean, Counsel to President Richard Nixon

Richard A. Epstein, Laurence A. Tisch Professor of Law, New York University Law School; Peter and Kristen Bedford Senior Fellow, The Hoover Institution; Senior Lecturer, University of Chicago Law School

Michael German, Senior Policy Counsel, American Civil Liberties Union; Special Agent, Federal Bureau of Investigation, 1988-2004; former Adjunct Professor, National Defense University School for National Security Executive Education

Philip Giraldi, Contributing Editor for *The American Conservative Magazine,* antiwar.com, and *Campaign for Liberty*; Executive Director, Council for the National Interest; former operations officer specializing in counter-terrorism, Central Intelligence Agency, 1975-1992; United States Army Intelligence

Asa Hutchinson, Senior Partner, Asa Hutchinson Law Group; Undersecretary, Department of Homeland Security, 2003-2005; Administrator, Drug Enforcement Administration, 2001-2003; Member of Congress (R-Ark.), 1997-2001; United States Attorney, Western District of Arkansas, 1982-1985

Mary O. McCarthy, Consultant, Freedom of Information and Privacy Act; Associate Deputy Inspector General, Investigations, Central Intelligence Agency, 2005-2006; Visiting Fellow, Center for Strategic and International Studies, 2002-2004; Senior Policy Planner, Directorate of Science and Technology, Central Intelligence Agency, 2001-2002; Senior Director, Special Assistant to the President, National Security Council, 1998-2001; Director for Intelligence Programs, National Security Council, 1996-1998; National Intelligence Officer for Warning, (Deputy 1991-1994) 1991-1996

James McPherson, Rear Admiral USN (Ret.); Executive Director, National Association of Attorneys General; Judge Advocate General of the Navy, 2004-2006; Deputy Judge Advocate General of the Navy, 2002-2004; Active Duty, United States Navy, Judge Advocate General's Corps, 1981-2006; former General Counsel for the Department of Defense Counterintelligence Field Activity

Paul R. Pillar, Visiting Professor and Director of Studies, Security Studies Program, Georgetown University; intelligence officer (positions included Deputy Chief of DCI Counterterrorist Center, National Intelligence Officer for the Near East and South Asia, and Executive Assistant to the Director of Central Intelligence), Central Intelligence Agency and National Intelligence Council, 1977-2005

Peter Raven-Hansen, Glen Earl Weston Research Professor of Law, The George Washington University Law School; Co-director, National Security and U.S. Foreign Relations Law Program

James Robertson, Neutral Arbitrator and Mediator, JAMS; U.S. District Judge for the District of Columbia, 1994-2010; Judge, Foreign Intelligence Surveillance Court, 1994-2005

William S. Sessions, Partner, Holland and Knight LLP; Director, Federal Bureau of Investigation, 1987-1993; Judge, United States District Court for the Western District of Texas, 1974-1987, Chief Judge, 1980-1987; United States Attorney, Western District of Texas, 1971-1974

Earl Silbert, Partner, DLA Piper; United States Attorney, District of Columbia, 1974-1979; former Watergate Prosecutor

Neal R. Sonnett, member, American Bar Association Board of Governors; Past Chair, American Bar Association Task Force on ABA Task Force on Treatment of Enemy Combatants and Task Force on Domestic Surveillance in the Fight Against Terrorism

Colby Vokey, Lieutenant Colonel USMC (Ret.); Attorney, Fitzpatrick Hagood Smith & Uhl LLP; Lieutenant Colonel, U.S. Marine Corps, 1987-2008; lead counsel for Guantanamo detainee Omar Khadar at Military Commissions, 2005-2007

John W. Whitehead, President, The Rutherford Institute

Lawrence B. Wilkerson, Colonel, U.S. Army (Ret.); Adjunct Professor of Government and Public Policy at the College of William and Mary; Chief of Staff to Secretary of State Colin L. Powell, 2002-2005

REPORTERS:

Jeffrey L. Cox, Orrick, Herrington, & Sutcliffe LLP

Andrew H. Erskine, Orrick, Herrington, & Sutcliffe LLP

Clifford R. Michel, Orrick, Herrington, & Sutcliffe LLP

THE CONSTITUTION PROJECT STAFF:

Sharon Bradford Franklin, Senior Counsel, Rule of Law Program

Jessica Neiterman, Fried Frank Fellow

* Affiliations are listed for identification purposes only