Paper Prepared for the 12th Workshop on the Economics of Information Security (WEIS 2013)

Georgetown University, Washington, D.C. June 11-12, 2013

Einstein on the Breach:

Surveillance Technology, Cybersecurity and Organizational Change

Milton Mueller and Andreas Kuehn

School of Information Studies, Syracuse University

mueller@syr.edu, ankuhn@syr.edu

Abstract

This paper explores the way cybersecurity technology alters organizational relationships. It is a case study of the implementation of intrusion detection and prevention technology (IDS/IPS) in U.S. government agencies, including the Einstein program and the Defense Industrial Base (DIB) Enhanced Cybersecurity Services (DIB/ECS) program. IDS/IPS employs deep packet inspection (DPI) capabilities to scan data packets in real-time and make decisions about how to handle incoming and outgoing network traffic based on automated recognition of threats. Drawing on the theory of the firm, we ask whether these cybersecurity initiatives led to more centralized, hierarchical control of Internet services and/or the internalization of functions and operations formerly provided by the private sector. We found that DPI implementations led to significant organizational changes in government agencies and threatened to blur the boundary between cybersecurity efforts confined to U.S government agencies and private sector ISPs, defense contractors and ISPs.

Keywords: Cybersecurity, Theory of the Firm, Transaction Cost Theory, Deep Packet Inspection, IDS/IPS, Internet Governance, Privacy, Surveillance.

1 Introduction

In May 2009, President Obama announced “a new comprehensive approach to securing America's digital infrastructure.” In the course of describing this new initiative, he stated that “Our pursuit of cybersecurity will not – I repeat, will not – include monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans.”[1] In the same speech, he also stated “Let me be very clear: My administration will not dictate security standards for private companies.”

Promoting security while avoiding surveillance or regulation of the private sector is proving to be more complicated and difficult than Obama’s speech let on. The Internet creates major interdependencies between the networks of government agencies and the networks supplied and used by the private sector. Additionally, the implementation of security technologies has an inherent tendency to alter lines of responsibility, management and control. Security technologies can, for example, create hierarchies where before there were market transactions or looser, networked forms of cooperation (e.g. Kuerbis and Mueller, 2011).

This paper is a case study of how cybersecurity technology implementation has altered, or threatened to alter, organizational relationships among civilian and military government agencies, Internet service providers, private businesses and users. As part of a larger project on the impact of deep packet inspection on Internet governance,[2] it examines the implementation of intrusion detection and prevention technology (IDS/IPS) by U.S. government agencies. Two federal cybersecurity initiatives involved DPI: 1) the ‘Einstein’ program, administered by the U.S. Department of Homeland Security (DHS) and 2) the Defense Industrial Base (DIB) Enhanced Cybersecurity Services (DIB/ECS) program initially administered by the U.S. Department of Defense (DoD).

IDS/IPS is intended to shield federal agencies against cyber-espionage, data exfiltration, malware, DDoS attacks and other network-based security threats. IDS/IPS employs deep packet inspection (DPI) capabilities to scan and analyze data flowing over networks in real-time. Based on automated recognition of threats, it issues alerts (IDS) or makes decisions about how to handle incoming and outgoing network traffic (IPS).

[1] The Whitehouse (2009). Remarks by the President on Securing Our Nation's Cyber Infrastructure. Office of the Press Secretary. May 29, 2009. – URL: http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure

[2] See http://deeppacket.info. In other research, we have argued that DPI is a potentially disruptive technology due to its clash with three pre-established principles of Internet governance: the end-to-end argument, users’ expectations regarding the confidentiality of their communication, and the legal immunities offered ISPs for the actions of their users. As a potentially disruptive technology, DPI may dramatically change the architecture, governance and use of the Internet. At the same time, it is also possible that DPI will be domesticated and regulated in ways that will make its use consistent with the principles and norms of the existing Internet. The research attempts to determine whether the use of DPI catalyzes changes in law, regulation and governance of Internet service providers, or whether those pre-established principles act to curb or limit the use of DPI.

Broadly, we are interested in the extent to which attempts to improve cybersecurity are leading to more state-based hierarchy and centralized control over the production of Internet access. The liberalization and privatization of telecommunications in the 1980s and '90s moved the supply of information and communication services, standards and equipment away from the state or state-delegated monopolies into a private sector-led, competitive market economy. The Internet accelerated this revolution by facilitating the creation and interoperability of an unprecedentedly large number of private data networks. The social, economic and cultural gains of this massive proliferation of devices and networks have been enormous. But those very same features make security initiatives vastly more complex. Hence, this case study investigates the way the federal government's implementation of cybersecurity policies and technologies altered organizational arrangements, not just inside the federal government itself, but also between the government and the private sector actors who supply it with Internet access and military products and services.

Drawing on theories of economic organization, specifically the theory of the firm, our research asks:

> How did the US federal government's cybersecurity initiatives alter the organizational arrangements among the federal agencies and the private sector parties with which they cooperated? To what extent did the uncertainties associated with cyber risks lead to more hierarchical control and the internalization of functions and operations formerly provided by the private sector?

We show that the implementation of cybersecurity policies and technologies led to reassessing and revising the roles and responsibilities of various actors. With respect to the first aspect of the RQ, we find that the federal government did consolidate Internet access and strengthen hierarchical control over federal agencies' Internet access. We also see efforts to extend surveillance and regulation to private, civilian networks, but document how political resistance and mistrust of government intelligence agencies prevented this in some cases and limited its scope in others.

2 Theory and Method

The theory of the firm provides a useful lens with which to analyze the organizational impact of federal cybersecurity initiatives, as it brings into relief many of the factors that created pressure for, and resistance to, organizational changes.

The *firm* is the economist's term for the basic decision making unit for production (Williamson & Winter, 1993). A variant of public choice theory considers the state to be a firm that supplies so-called 'public' goods[3] (Auster & Silver, 1979; Forte, 2010). Like a firm, the state draws on information, technology and its own managerial capabilities to combine factors of production into the types and quantities of

[3] We use the term 'public goods' reluctantly because of the huge disjunction between the formal economic definition of a public good and the goods that states actually provide. Many if not most of the services the state provides do not qualify as public goods, in that they are neither nonrival in consumption nor non-exclusive. Colloquially, however, it has become common to deem anything the state provides as a public good precisely because the state provides it.

services society signals that it wants the state to produce. Demand for the state's services however is conveyed not through the market price system but through political mechanisms such as voting, lobbying, political campaigns, rent-seeking and so on.

2.1 Transaction Costs

A major preoccupation of firm theory has been to explain what is produced within an organization (in-sourced) and what goods and services are acquired across firms through markets or contractual agreements (out-sourced). Transaction costs (TC) are the costs of engaging in the search, negotiation, monitoring and enforcement needed to support a market exchange, whereas management costs (MC) are the equivalent costs associated with supervising the execution of the task internally. *Ceteris paribus*, the lower TC relative to MC, the more organizations will tend to acquire goods and services from other firms as opposed to making them within the organization; conversely, the higher TC relative to MC, the more likely they will be internalized in a hierarchical organization. Hierarchy can be used to resolve differences among actors via managerial fiat, as well as to gain access to information that would otherwise not be available. Production costs, and especially the presence or absence of scale economies, is another significant factor affecting the boundaries of the firm.[4]

Governments, like private firms, are constantly faced with the question of which functions and services to in-source and which to out-source. Research and policy work in public administration emphasizes the way outsourcing to more specialized, efficient private firms can reduce governments' costs while retaining and even enhancing their role in public policy implementation; there is also some literature on the reversal of privatizations (e.g., Warner and Hefetz, 2012).

Cybersecurity presents a complex picture with respect to in-sourcing and out-sourcing. One potentially relevant strand of TC theory emphasizes the way in-sourcing can eliminate uncertainty about the supply of or access to a required input. By taking direct control of security management, the government can be more certain that it is actually achieving security objectives that have become politically salient. Deep, operational knowledge of the specific configuration and architecture of a network might also be considered a form of asset specificity, which would militate against outsourcing. On the other hand, computer and network security operations clearly involve forms of expertise that might be best concentrated in specialized firms and acquired through outsourcing. Research in this area emphasizes how performance-based contracts can reconcile a managed security services provider's incentive to shirk and their need to maintain a good reputation to remain competitive (Ding, Yurcik and Xin, 2005).

2.2 Public vs. Private Security

One of the benefits of a firm-theoretic approach is that it highlights and clarifies an important distinction between two aspects of the federal government's pursuit of cybersecurity. On one hand, the government can act to improve the security of its *own* networks. In this respect security is pursued as a private good, not much differently than a private firm. On the other hand, the government can try to

[4] As Demsetz (1993) has noted, even if transaction costs are zero, a good or service might still be produced by a firm if there are increasing returns to scale, as demand for additional units of the good can more efficiently be met by expanding a firm's output as opposed to purchasing the service from diverse smaller suppliers in a market.

provide Internet security as a public good for the country as a whole.[5] The two objectives, though interrelated, must be kept distinct. The organizational arrangements that might optimize security for the federal government's own systems are not necessarily the same as those required for optimizing security across the Internet as a whole. Indeed, in this case study we can see tensions between those two agendas in play.[6]

The internally-oriented federal cybersecurity initiatives described below consisted largely of getting a diverse set of agencies and departments to participate in new, centrally-directed, common security arrangements. On the whole, security management responsibility for the government's own networks seems to have been drawn inward and made more hierarchical and coordinated. Governmental efforts to promote cybersecurity as a public good, on the other hand, had important implications for private sector suppliers of Internet access and the general public. Efforts by the military and the NSA to apply IDS/IPS to the public 'critical infrastructure' would have created new forms of surveillance or supervision of the private sector by the US government. There was, as we shall see, significant resistance to that. The shifting of these boundaries is an accelerated repetition and temporal extension of what Myriam Dunn Cavelty described as a *threat frame,* that broadens the threat landscape from U.S. government networks to critical infrastructure and finally to the entire society. Consequently, the distinction between internal and external threats and private and public spheres of action becomes contentious (Dunn Cavelty, 2008). While those boundaries are shifted and threats and enemies remain ambiguous, cybersecurity and national security tend to meld due to calls to use the military/intelligence expertise and capabilities to secure both U.S. government networks and public infrastructure.

2.3 Method

This research follows a case study approach (Eisenhardt, 1989; Yin 2008). To understand the organizational impact of the IDS/IPS initiatives, we first systematically reviewed the documentary evidence of the federal government's cybersecurity policy initiatives after 9/11. This included the high-level executive orders and presidential directives as well as the legally-required privacy impact assessments filed regarding the Einstein program. We also conducted interviews with technology vendors, government officials, academics and activists involved in these initiatives during the summer of 2012. We categorized the Einstein program into 3 phases. Phase 1 corresponds to the implementation of Einstein 1; phase 2 to the implementation of Einstein 2. Phase 3, which involved the third iteration of the Einstein program, we classify as a period of "blurred boundaries" between the government and the private sector. It includes the DIB/ECS program as well as Einstein 3 and focuses on the expansion of IDS/IPS into the private sector.

[5] The idea of 'cybersecurity in one country' is probably an oxymoron; any attempt to provide cybersecurity as a public good would probably have to entail transnational efforts.

[6] Public and private security can be complements. While security is generally considered a public good and one of the primary functions of the state, it is also true that *both* public and private goods are usually employed to fulfill the public's demand for security. Protection against crime, for example, is provided by bodyguards, watchdogs, alarms and locks as well as by the police. Abstract arguments that security is a public good tell us very little about which mix of public and private security measures is optimal.

To track the first aspect of the research question, we have broken down the basic elements of government agency Internet access into a simplified list of component parts. For each of the phases noted above, we schematized the extent to which they were in-sourced and out-sourced. Tables with these schemata are found at the end of each section. Additionally, in the next section we explain more specifically the key economic components of an IDS/IPS system, and discuss the various modes of economic organization that might be associated with its implementation.

3 DPI and the Firm

Deep packet inspection (DPI) is a technology for scanning and analyzing Internet traffic and making decisions about how to handle it in real-time. It is an enabling technology that can be used for many different applications. For instance, in addition to detecting and blocking network security threats through IDS/IPS applications, it can be used to prevent exfiltration of private or classified information, for censorship and surveillance, for bandwidth management, for copyright policing, and for online behavioral advertising (Mueller & Asghari, 2012; Mueller, Kuehn, & Santoso, 2012; Kuehn & Mueller, 2012).

DPI capabilities were first developed for intrusion detection and prevention systems. Intrusion detection systems (IDS) allowed network operators to passively detect incoming or outgoing traffic associated with recognized forms of malware (viruses, Trojans, worms, and other dangerous code). Intrusion prevention systems (IPS) utilize IDS but supplement its recognition capabilities with programmed actions that stop or block the intrusion (Sourdis, 2007). Both IDS and IPS are based on signatures, a predefined set of values that describes a particular pattern in the network traffic. If the signature matches a particular pattern associated with malware or attacks, predefined actions are triggered. An IDS merely recognizes and reports suspect network activities, whereas an IPS takes automated actions to stop them. Thus, signature-based IDS/IPS can only prevent attacks previously known to the signature provider. Appendix B contains a sample signature.

In organizing the implementation of a DPI capability, one must make decisions about two key aspects of the system. First, what is the source of the signatures that will be used to detect threats? Second, where will the DPI box itself be situated and who will be responsible for operating it?

With respect to the signatures, a number of options regarding the production and sharing of threat recognition information are possible. The government can produce its own signatures. Conversely, the government could stay out of signature production altogether and rely on private sector actors to produce signatures. Or there could be a mixed regime, with a variety of sources producing signatures. Aside from who produces them, there is the issue of how signatures are distributed or shared. The various parties can pool the signatures and share them freely, restrict their distribution, or share some and restrict others. We try to encapsulate these as nine options in the simplified matrix in Table 1; the darkened cell shows where we are in the real world.

As the empirical evidence will show, the production and sharing of threat information was a key point of negotiation and concern in the organization of cybersecurity implementations. Open sharing of

Table 1: Possible methods of organizing IDS/IPS signature production

Signature producer	*Shared*	*Not Shared*	*Mixed*
Government			
Private Sector			
Both			▨

signatures makes the most efficient use of a nonrival informational resource and may have good security results; however, the NSA insisted on keeping some of its signatures classified in order to prevent adversaries from knowing that it recognizes its exploits. Reliance on military or intelligence agency signatures and threat information would benefit from the specialized expertise of the agencies, but could also restrict sharing and use of the signatures, which can create its own set of security pathologies. There might also be a less than perfect match between the signatures produced by military and intelligence agencies and the actual threats and vulnerabilities routinely faced by the private sector and the public. In an environment of secrecy there is also the possibility of abuse of the signature production function for unlawful surveillance purposes.

Decisions about the operation of the DPI box also have significant implications for both efficiency and security. Is it located in the public ISP, where it can inspect traffic from any user, or is it confined to the organizational gateway of the government agency? Is the box administered by the ISP, or by the individual government agency at its link to the Internet, or by a centralized government agency working across multiple gateways and agencies? How are the signatures fed into the machine and how are they updated? If some signatures are classified special procedures must be in place to shield the information and restrict distribution. What are the policies that specific threat recognition alarms will trigger? How widespread are the notifications? Who must take action based on the notification? The empirical evidence below will show that these issues, too, loomed large in the implementation of the Einstein and DIB/ECS programs.

Due to privacy law considerations, the creation of signatures for the Einstein program follows a review process that addresses personally identifiable information (PII). PII can only be used upon approval and to detect targeted threats. The procedures in place are supposed to avoid the collection of irrelevant network traffic.[7] Bellovin et al. (2011) discussed the architecture and limitations of IDS/IPS systems, using the U.S. example of the Einstein 3 program.

4 Cybersecurity policy and technology

In response to the developing threat landscape, intense policy making efforts took place over the last two Presidential administrations to improve the security cyberspace. What follows is a brief account of the major policy decisions and related technology deployments. Appendix C contains a timeline that depicts the major elements of the policy development.

[7] DHS (2012). Privacy Compliance Review of the EINSTEIN Program. January 3, 2012 – URL: http://www.dhs.gov/xlibrary/assets/privacy/privacy_privcomrev_nppd_ein.pdf

4.1 Policy Development

Our narrative begins with the 9/11 terrorist attacks in the U.S., which greatly affected both cyber- and physical security policy. In 2002, a secret executive order signed by then President George W. Bush authorized the National Security Agency (NSA) to deploy DPI to intercept and inspect telecommunication and Internet networks without a court warrant. Domestic as well as foreign traffic was included in its scope. Deep packet inspection equipment was secretly installed at major network nodes with the cooperation of private U.S. telecom firms AT&T, Verizon and BellSouth.

Monitoring domestic communication contravened NSA's governing law, the Foreign Intelligence Surveillance Act of 1978, (FISA). Once the program was exposed by a whistleblower, it fueled fears that the NSA's spying capabilities were also directed towards American citizens and domestic communication. (Klein, 2009; Wu, 2010: 238; Landau, 2010: 2) Fears and concerns about NSA involvement in cybersecurity efforts stemming from the warrantless wiretapping program played an important role in future negotiations over the Einstein program.

With the creation of the Department of Homeland Security (DHS) in late 2002, a "National Strategy to Secure Cyberspace" was issued.[8] The Bush administration put forward a bottom-up approach by coordinated efforts with state and local governments and the private sector to address cybersecurity policy issues and challenges (Harknett & Stever, 2011). In the same year, the Federal Information Security Management Act (FISMA, 44 U.S.C. § 3541, et seq.) was enacted. FISMA required all federal agencies to implement effective information security controls to protect information and information systems. In late 2003, the DHS became responsible for coordinating plans to protect critical infrastructure.[9] In September 2003, the United States Computer Emergency Readiness Team (US-CERT) was formed as a partnership between the DHS and the private sector to coordinate response to Internet security threats. The Federal Computer Incident Response Center (FedCIRC) located at the General Service Administration (GSA) was the US-CERT's predecessor with similar duties: response coordination, incident reporting and sharing of vulnerability information across the federal agencies.[10]

4.2 Einstein 1: Early Monitoring Capabilities

The organized deployment of federal government-wide cybersecurity monitoring capabilities began in 2003 when US-CERT, the operational arm of the Department of Homeland Security's National Cyber Security Division (NCSD), developed and initiated the Einstein program.[11] The objectives of Einstein 1 were to improve cyber threat monitoring and response capabilities at civilian federal government agencies by generating and sharing better information about network activity. For the agencies who

[8] DHS (2003). National Strategy to Secure Cyberspace. February, 2003. – URL: http://www.dhs.gov/files/publications/editorial_0329.shtm.

[9] DHS (2003) Homeland Security Presidential Directive-7 (HSPD 7). Critical Infrastructure Identification, Prioritization, and Protection. December 17, 2003. – URL: http://www.dhs.gov/homeland-security-presidential-directive-7

[10] Dacey (2002). Critical Infrastructure Protection, Significant Homeland Security Challenges Need to Be Addressed. Testimony of Robert F. Dacey before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives, July 9, 2002. – URL: http://www.gao.gov/assets/110/109467.pdf

[11] DHS (2010). Privacy Impact Assessment Update for the EINSTEIN 1: Michigan Proof of Concept. February 19, 2010 – URL: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_einstein1michigan.pdf

installed a sensor, Einstein 1 automatically collected network flow information at Internet gateways, allowing US-CERT to correlate and analyze it to detect anomalies that might indicate security threats. Network flow information includes the sending and receiving IP addresses, the sending and receiving port numbers, a number indicating the protocol used, the number of packets and bytes sent, the start and end time of the connection, the name of the sensor that collected the information, and a few other items. Appendix A contains a more detailed explanation and example of a flow record.

In firm-theoretic terms, Einstein 1 established a specialized functional capability (US-CERT) within the civilian federal agencies. Flow records indicating malicious activities were sent to US-CERT for further investigation, which could then (in theory) coordinate threat mitigation with associated government networks and share network security information with the public and private sectors. But this was a passive data collection capability; it created records that could be shared and analyzed by experts but did not fully leverage the state-firm's hierarchical organizing capabilities. Agency participation in the program was voluntary. Adoption by federal agencies remained at a low level, which was predictable given the budget and time constraints affecting agency managers. As of 2005, only three agencies had deployed Einstein 1; as of December 2006, the circle of participating agencies had expanded to only eight out of several hundred.[12] Furthermore, even though information was being collected, the procedures for sharing it in real time and for developing coordinated responses were not well developed. Neither the technology nor the organizational arrangements behind Einstein 1 automated response mechanisms. Finally, the initiative was confined to the civilian agencies and was not integrated or well-coordinated with the capabilities of military and intelligence agencies.

4.3 Einstein 2 and the Trusted Internet Connection Program

Phase Two of the state-firm's response involved greater consolidation of Internet access and greater automation and centralization of monitoring and control. In late November 2007, under the auspices of the Office of Management and Budget (OMB) and the DHS, a federal government-wide initiative known as the Trusted Internet Connections (TIC) program was instituted. TIC was aimed at consolidating external network access points and improving their security.[13] Up to this point, federal agencies could autonomously transact for their own Internet connections. The number of such connections was approaching 5,000. The original target was to reduce the number by a factor of one hundred, to fifty approved external access points.[14] The initial deadline for the TIC implementation across the federal

[12] DHS (2007) Challenges Remain in Securing the Nation's Cyber Infrastructure. Office of the Inspector General (OIG-07-48, June 2007) - http://web.archive.org/web/20090326172325/http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07-48_Jun07.pdf

[13] "All federal agencies in the executive branch, except for the Department of Defense, are required to implement the initiative". In: GAO (2010). Information Security - Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies. March, 2010; GAO 10-237. – URL: http://www.gao.gov/new.items/d10237.pdf

[14] OMB (2007). Memorandum M ‐ 08-05, Implementation of Trusted Internet Connections (TIC). OMB, November 20, 2007. – URL: http://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2008/m08-05.pdf; As of January 2008, 4300+ connections existed; this number was reduced by May 2008 to 2758; the target number of connections is smaller or equal 100. In: DHS (2008). Trusted Internet Connections (TIC) Initiative, Statement of Capability Evaluation Report. June 4, 2008. – URL: http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/2008_TIC_SOC_EvaluationReport.pdf

government was June 2008, but was later postponed to December 2009.[15] From a network security perspective, there are two reasons to consolidate external network connections: 1) a smaller number of external access points can be centrally monitored more easily and offers adversaries fewer targets for security exploits; and 2) the TIC locations can be used to deploy an IDS/IPS capability more economically. Aside from a few exceptions, the TIC program required external connections to be routed through approved TIC access points.[16]

The major formal policy milestone in the U.S. debate on cybersecurity came in January 2008 with the still-classified Comprehensive National Cybersecurity Initiative (CNCI).[17] CNCI was based on National Security Presidential Directive 54 *Cyber Security and Monitoring* (NSPD 54) which was also referred to as Homeland Security Presidential Directive 23 *Cyber Security and Monitoring* (HSPD 23). The CNCI set in motion a dozen initiatives, centralized earlier efforts and integrated the Einstein Program's progression towards IDS and IPS and the TIC Program's progression towards a lower number of external network gateways. Under CNCI, federal agencies can only obtain Internet access in four ways: 1) by becoming a TIC access provider (TICAP) after successful certification and providing their own access service; 2) by seeking access from another TICAP; 3) by obtaining access through an approved commercial provider through a Managed Trusted IP Service (MTIPS) or 4) some hybrid of the above.[18] Figure 1 shows the four options.[19] The vast majority of agencies get access through a TICAP.[20] Commercial service providers ("Networx vendors") provide flexibility in obtaining access services; most agencies indicated that they will obtain managed security capabilities as part of their TIC implementation. [21] Small agencies may share TICs, while larger agencies may need several secured external Internet gateways.

The CNCI's vision was to manage the federal government's civilian agency networks as a single network. Concerns about privacy and civil liberties arose because CNCI remained classified. Briefly after CNCI was issued, public and closed Congressional hearings took place.[22] Newly-elected President Obama's Cyberspace Policy Review provided key recommendations with regards to CNCI and assured that

[15] GAO (2010). Information Security - Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies. March 12, 2010; GAO 10-237. – URL: http://www.gao.gov/new.items/d10237.pdf

[16] Ibid.

[17] A summary of the CNCI was declassified by the Obama Administration in 2010. See: The White House (2010), http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf

[18] Ibid.

[19] GAO (2010). Information Security - Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies. March 12, 2010, GAO-10-237. – URL: http://www.gao.gov/products/GAO-10-237

[20] As of 2008, 144 federal agencies (35% of solicited agencies) reported that 82% will seek service, where as 15% will provide single service and 3% will provide multi service. In: DHS (2008). Trusted Internet Connections (TIC) Initiative, Statement of Capability Evaluation Report. June 4, 2008. – URL: http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/2008_TIC_SOC_EvaluationReport.pdf

[21] Ibid.

[22] U.S. H.R. Homeland Security Committee, hearing 'The Cyber Initiative' on February 28, 2008. – URL: http://web.archive.org/web/20080326202649/http://homeland.house.gov/Hearings/index.asp?id=118; and U.S Senate Homeland Security & Governmental Affairs Committee, classified hearing 'NSPD-54/HSPD-23 and the Comprehensive National Cybersecurity Initiative' on March 4, 2008. – URL: http://web.archive.org/web/20080325202700/http://hsgac.senate.gov/index.cfm?Fuseaction=Hearings.Detail&HearingID=528.

attention was given to privacy rights and civil liberties. [23] The incoming Obama administration also addressed complaints about the previous administration/DHS's approach to taking too long. Consequently, the new administration shifted its policy efforts to what Harknett & Stever (2011) described s as a top-down, rational, comprehensive approach by putting the White House in charge of cybersecurity. An early 2008 TIC evaluation report articulated the need for coordination regarding implementation of technical requirements, including "deep packet inspection of encrypted sessions, storage volume requirements, uniform time services, the sharing and use of custom IDS signatures, and Sensitive Compartmentalized Information Facility (SCIF) requirements." It also addressed the Einstein deployment and international TIC locations.[24]

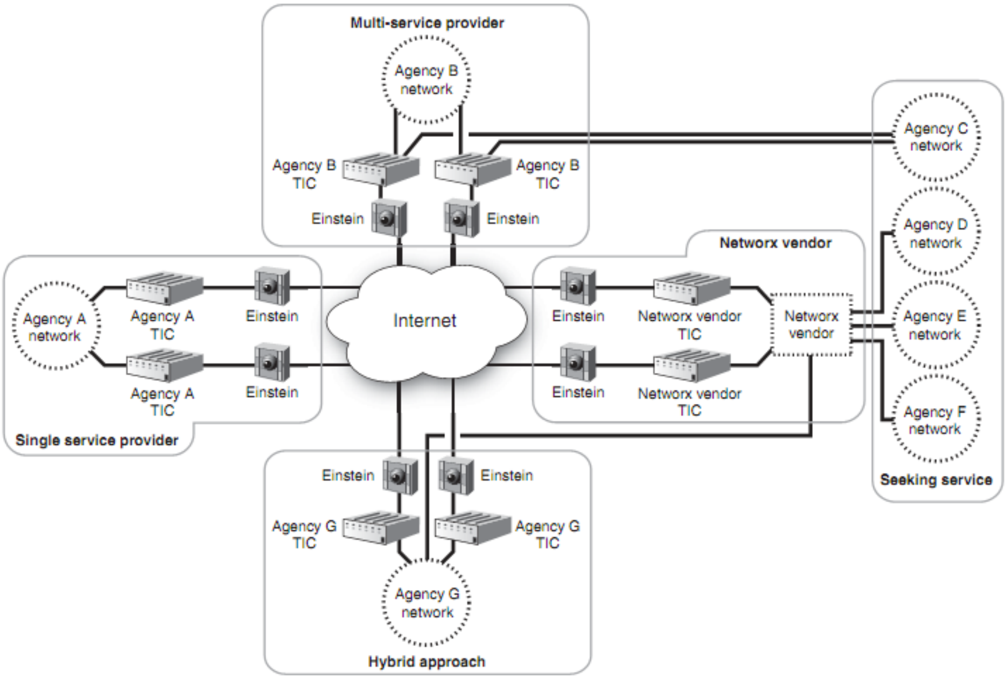


Figure 1: TIC access service options – Interaction of TIC and Einstein (Source: GAO-10-237)

Based on IP address ranges, traffic is monitored to identify malicious traffic by deploying signature-based and anomaly-based IDS at the agency's TIC gateways. The scanning is not directly in-line; a temporary copy of the traffic is created and scanned for suspect patterns.[25] As Bellovin et al. (2011) observed, cutting the number of external access points was a crucial prerequisite for the Einstein 2 capability. It cut down the number of monitoring points, allowing more expensive and sophisticated

[23] The White House (2009). Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure. – URL: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf. See related documents, URL: http://www.whitehouse.gov/cyberreview/documents; and Rollins, John & Henning, Anna, C. (2009) Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations. Congressional Research Service, March 10, 2009 – URL: http://www.fas.org/sgp/crs/natsec/R40427.pdf

[24] Ibid.

[25] Bradbury, Steven G. (2009) 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. DoJ, Opinions of the Office of Legal Counsel, in Vol. 33 (January 9, 2009). – URL: http://www.justice.gov/olc/2009/e2-issues.pdf

detection technology to be deployed at those points. But it also posed challenges; the new gateways had to be secure and scalable enough to handle higher levels of network traffic; the routing architecture also had to be modified.[26]

Einstein 2 strengthened US-CERT's ability to surveil security incidents across federal civilian networks. Its facilities combined commercial, off-the-shelf and government-developed technology. It deployed an intrusion detection system that used DPI capabilities to scan for malicious activities in incoming and outgoing network traffic. Most of the network data scanned by Einstein 1 was contained in the packet header, but Einstein 2 looked inside the payload of the packet for signatures of threats. The ability to detect network security threats is based on a predefined set of custom signatures that formally describe malicious network traffic.[27] If a signature matches a specific network traffic pattern, US-CERT is alerted (e.g. a specific email attachment that contains a computer virus might trigger such a notice).

As of September 2009, none of the 23 reviewed agencies had met all TIC requirements. Sixteen agencies that opted to provide access themselves cut down the number of external access points from 3,286 to approximately 1,753.[28] Similarly, agency participation in the Einstein effort lagged at the outset. Subsequently, Einstein 2 was made mandatory for all federal agencies, as part of a push to gain situational network security awareness.[29] Notably, the Department of Defense and intelligence agencies were exempted from the Einstein program, as they already had their own IDS capabilities. As of September 2009, Einstein 2 was deployed at six agencies.[30] In 2011, 15 agencies providing Internet access and four private telecommunications service providers (Managed Trusted Internet Protocol Services) had fully deployed and activated Einstein 2.[31]

4.4 Blurring Boundaries

In Phase 3, attention shifts from government agencies to the relationship with the private sector. The overlap and tensions between the federal government's narrower requirement to secure its own networks and its broader mandate to provide cybersecurity as a general public good create a period of confusion and negotiation. There were criticisms aired that the information sharing between the public and private sector were not working. There were "research" initiatives that toyed with the idea of placing government-operated sensors to detect malicious network activities in private sector infrastructure. The NSA's role as a provider of threat signatures became more openly asserted and generated political concern. The federal government's cybersecurity efforts were extended to private

[26] Juniper Networks (2008). Juniper Networks Trusted Internet Connection (TIC) Solution. – URL: http://www.juniper.net/us/en/local/pdf/solutionbriefs/3510299-en.pdf

[27] DHS (2012). Privacy Compliance Review of the EINSTEIN Program. January 3, 2012 – URL: http://www.dhs.gov/xlibrary/assets/privacy/privacy_privcomrev_nppd_ein.pdf

[28] GAO (2010). Information Security - Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies. March 12, 2010, GAO-10-237. – URL: http://www.gao.gov/products/GAO-10-237

[29] OMB (2007). Memorandum M - 08-05, Implementation of Trusted Internet Connections (TIC). OMB, November 20, 2007. – URL: http://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2008/m08-05.pdf

[30] GAO (2010). Information Security - Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies. March 12, 2010, GAO-10-237. – URL: http://www.gao.gov/products/GAO-10-237

[31] GAO (2011). Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11. GAO-11-881, September 7, 2011. – URL: http://www.gao.gov/products/GAO-11-881

firms in the so-called Defense Industrial Base (DIB). In this phase, the control of cybersecurity information and monitoring capabilities are re-negotiated among the public and private sector and, within the federal government, between the military and civilian branches. In this section we try to describe and explain the equilibrium that was reached.

4.4.1 Role of NSA

The NSA, a military agency, took the lead in pushing a more expansive approach toward the achievement of public security, involving a stronger role for government in producing technology for the private sector and in monitoring private infrastructure. In September 2007 the *Baltimore Sun* newspaper revealed that Director of National Intelligence Mike McConnell, a former NSA chief, was coordinating a highly classified 'Cyber Initiative' with NSA, DHS and unspecified 'other federal agencies' to monitor civilian networks for unauthorized intrusions.[32] This foray into securing domestic private communications would be a significant change in NSA's role, which was supposed to be confined to foreign targets. Coming not long after public exposure of the warrantless wiretapping program in late 2005, fears of privacy violations and government surveillance were aired. As Landau (2010: 119) pointed out, when asked "how do you protect civilian networks without observing the traffic on them?" the administration was not forthcoming with an answer. The *Baltimore Sun* story was the first indication that efforts to secure cyberspace were not limited to U.S. government networks.

The NSA's role in domestic wiretapping was also demonstrated in the summer of 2007, when the controversial Protect America Act (PAA) (Pub. L. 110-055) was passed, making significant changes to FISA. A retroactive attempt to legalize what the Bush administration had done years before, PAA allowed warrantless wiretapping if it was "reasonably believed" that one end was outside of the U.S. (Bellovin et al., 2008). In the meantime, an AT&T switching office in San Francisco was exposed as being involved in redirecting domestic traffic to NSA. (Wolfson, 2007-08; Mossavar-Rahmani, 2008; Landau, 2010: 2)

Continuing in this vein, the summer of 2010 saw the NSA award a classified contract worth up to USD 91 million and lasting at least through September 2014 to defense contractor Raytheon regarding protection of critical infrastructure. [33] The project, named "Perfect Citizen," was to study sensors in critical infrastructure to detect malicious network activities, particularly utilities and the electrical power grid. Where the Einstein program focused on shielding federal communications networks, Perfect Citizen targeted sensitive control systems (SCS) or industrial control systems (ICS), including communications for supervisory control and data acquisition (SCADA) used for automated control and data collection of distributed utilities.[34] Of particular concern were control systems that were originally

[32] Gorman, Siobhan (2007). NSA to Defend Against Hackers: Privacy Fears Raised as Spy Agency Turns to System Protection. Baltimore Sun, September 20, 2007. – URL: http://articles.baltimoresun.com/2007-09-20/news/0709200117_1_homeland-national-security-agency-intelligence-agencies

[33] Gorman, Siobhan (2010). U.S. Plans Cyber Shield for Utilities, Companies. The Wall Street Journal, July 8, 2010. – URL: http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html; and NSA (2012). FOIA Case 62332B, December 18, 2012. "Statement of Work for (U) PERFECTCITIZEN. September 8, 2009". – URL: http://epic.org/foia/nsa/NSA-PerfectCitizen-FOIA_Docs.pdf

[34] NSA (2010). A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS). Systems and Network Analysis Center. Version 1.1, August 20, 2010. – URL:

designed as independent, stand-alone units but were later connected to the Internet, sometimes without adopting necessary security requirements. Just as the prospect of extending Einstein 3 to the public Internet drew critical reaction, negative public reaction to Perfect Citizen forced NSA to respond that these were purely research efforts; real sensors would not be placed nor networks monitored in the private sector.[35]

4.4.2 "The Exercise"

In 2010 an attempt was launched to add intrusion prevention (IPS) capabilities to the existing IDS capabilities of the Einstein program. Like IDS, IPS makes use of deep packet inspection technology, but not only identifies but also acts upon predefined threat signatures. IPS was considered the third phase of the Einstein program.

A small-scale trial of IPS, referred to as "The Exercise" in government memos, was conducted. A commercial Internet Service Provider (ISP) provided with Einstein capabilities redirected traffic to and from an undisclosed, single medium-sized federal civilian agency.[36] In the beginning of Einstein 3, in particular during "The Exercise", commercial and government technologies were combined at the agency TICAPs; the trial used NSA-developed IPS technology. The network traffic in question was routed from the agency's TICAPs to a secured room within the access provider where the DHS itself operated the government-owned IPS boxes. After the network traffic passed through the intrusion prevention devices, it was directed back to the participating agency.[37]

As the federal government stood poised to implement Einstein 3 in full, fears were expressed by some prominent technical experts that government-controlled Einstein IDS/IPS capabilities would be extended into the private sector infrastructure (Bellovin et al., 2011). The legacy of mistrust generated by the NSA contributed to these fears. These kinds of concerns tended to push the administration to bring the civilian agency (DHS) into the lead over NSA as the intermediary between the private sector and the government in federal cybersecurity efforts. While early instances of Einstein 3 relied heavily on government furnished equipment, in later instances technology use shifted significantly to ISP owned and operated equipment for active monitoring. Direct NSA participation was reduced and only the DHS deployed signatures.

4.4.3 Government-Private Sector Sharing of Information

The issue of how information generated by IDS/IPS would be shared posed another area of blurred boundaries between the public and private sectors. As the Einstein program progressed, one report recommended DHS to evaluate "the feasibility of sharing federally developed technology capabilities"

http://www.nsa.gov/ia/_files/ics/ics_fact_sheet.pdf; and NSA (2012). FOIA Case 62332B, December 18, 2012. Further, US-CERT has a specialized program, the Control Systems Security Program (CSSP), that addresses control systems within the nation's critical infrastructure, the Industrial Control Systems CERT (ICS-CERT). – URL: http://ics-cert.us-cert.gov

[35] Singel, Ryan (2010). NSA Denies It Will Spy on Utilities. Wired, Threat Level, July 9, 2010. – URL: http://www.wired.com/threatlevel/2010/07/nsa-perfect-citizen-denial

[36] DHS (2010). Privacy Impact Assessment for the Initiative Three Exercise. March 18, 2010. – URL: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3exercise.pdf

[37] Ibid.

with critical infrastructure providers.[38] An independent GAO report in 2010 unveiled crucial issues in the sharing of security incident information. It concluded that public-private partnerships intended to exchange timely and actionable cyber threat information were not working.[39] While federal agencies were not meeting private sector expectations, some private companies were not willing to share sensitive, proprietary information with the government. A related 2008 GAO report had identified these challenges two years earlier, but was met with little interest.[40] However, a report from the DHS' Inspector General revealed that even the sharing of cyber threat information coming out of Einstein was marginal. Einstein was called an "effective tool" while US-CERT was said to be "unable to share near real-time data and classified and detailed information to address security incidents."[41]

Einstein information is shared only within DHS; otherwise a Memorandum of Agreement is required. In early 2012 it was reported that international information-sharing agreements with Israel and India existed, US-CERT shared information with these two governments through the use of Einstein 2 technology.[42] Other DHS partnerships on cybersecurity with foreign governments, including Australia, Canada, Egypt, the Netherlands, and Sweden, have existed since 2009. [43]

4.4.4 Extending Network Protection to Defense Contractors

Network protection efforts were also extended into the private sector through the Department of Defense, based in part on the evolving Einstein model. The networks and information systems of military contractors, known in Washington as the Defense Industrial Base (DIB) companies, contain sensitive U.S. military information and intellectual property, and have been repeatedly targeted in cyberattacks. In 2011, the Department of Defense conducted a pilot, referred to as DoD Defense Industrial Base Opt-in Pilot Exploratory Cybersecurity Initiative, under its DIB Cyber Security/Information Assurance (CS/IA) Program. During the 90-day voluntary pilot, Tier 1 Internet service providers deployed signatures

[38] DHS (2010). Privacy Impact Assessment Update for the EINSTEIN 1: Michigan Proof of Concept. February 19, 2010. – URL: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_einstein1michigan.pdf

[39] GAO (2010). Critical Infrastructure Protection - Key Private and Public Cyber Expectations Need to Be Consistently Addressed. GAO-10-628, July 15, 2010 – URL: http://www.gao.gov/products/GAO-10-628

[40] GAO (2008). Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability. GAO-08-588, (Washington D.C.: July 31, 2008). – URL: http://www.gao.gov/products/GAO-08-588

[41] Statement of Richard L. Skinner, Inspector General, DHS before the H.R. Committee on Homeland Security, June 16, 2010. – URL: http://web.archive.org/web/20100805235526/http://www.dhs.gov/xoig/assets/testimony/OIGtm_RLS_061610.pdf; and DHS (2010). U.S. Computer Emergency Readiness Team Makes Progress in Securing Cyberspace, but Challenges Remain. Office of Inspector General. OIG-10-94, June 2010. – URL: http://web.archive.org/web/20100705034034/http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_10-94_Jun10.pdf

[42] DHS (2012). Privacy Compliance Review of the EINSTEIN Program. January 3, 2012. – URL: http://www.dhs.gov/xlibrary/assets/ privacy/privacy_privcomrev_nppd_ein.pdf

[43] Statement of DHS Secretary Janet Napolitano before the U.S. Senate Join Hearing before Committee on Commerce, Science, and Transportation and Committee on Homeland Security and Governmental Affairs on "The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting Our National and Economic Security", March 7, 2013. – URL: http://www.dhs.gov/news/2013/03/07/written-testimony-dhs-secretary-janet-napolitano-senate-committee-homeland-security

provided by the NSA to monitor the participating DIB companies' networks.[44] The pilot contained network prevention capabilities, analogous to Einstein 3 but not in its full extent; as a senior DoD official stated "[…] by way of analog, it [DIB Opt-in Pilot] is looking for part of the dot-com to bring what Einstein 3 is supposed to bring to dot-gov."[45] According to a *Washington Post* article, AT&T, Verizon, and CenturyLink took part in this pilot to protect the networks of 15 defense contractors, among them Lockheed Martin, SAIC and Northrop Grumman.[46] While the DIB companies obtained a higher degree of network security, network traffic monitoring was conducted by the ISPs, not DoD. The contractors were not required to report cybersecurity incidents detected during the DIB Opt-in Pilot to DoD.

In January 2012, it was announced that the Pentagon handed over the DIB Opt-in Pilot to the DHS to jointly undertake another proof of concept. Consequently, the pilot was renamed the "Joint Cybersecurity Services Pilot (JCSP)" but participation in it remained voluntary. The operational relationships with the Internet service providers were shifted to DHS. Henceforth, DHS furnished unclassified and classified indicators to the Internet service providers which converted those into machine-readable signatures for their intrusion detection and prevention systems. DHS continued the two cyber threat countermeasures in the JSCP that were already in operation at the Pentagon pilot, deployed at the Internet service provider site: first, the DNS sinkholing (if a signature matches outbound DNS requests to a known, malicious domain (e.g. botnets, spyware), this traffic is redirected to a "sinkhole server", effectively blocking DNS communications); and second, e-mail filtering (if a signature matches an infected attachment of an incoming e-mail, the messages is quarantined)[47]

After the 6-month joint proof of concept was completed, it was turned into a voluntary program. The "Joint Cybersecurity Services Program" (JSCP) was opened up to all of the more than 200 eligible DIB companies in May 2012.[48] JSCP became the optional component known as the DIB Enhanced Cybersecurity Services (DECS) in the Defense Department's voluntary cyber threat information and best practices sharing efforts (CS/IA) program. DHS acted as a point of contact for the participating Internet service providers – AT&T and CenturyLink –offering Einstein3-like capabilities, while DoD managed the relations to the DIB companies.[49] DoD lacked the authority to require DIB companies to participate in

[44] DoD (2011) Privacy Impact Assessment for the Defense Industrial Base (DIB) Cyber Security/Information Assurance Activities. – URL: http://dodcio.defense.gov/Portals/0/Documents/DIB%20CS-IA%20PIA_FINAL_signed_30jun2011_VMSS_GGMR_RC.pdf

[45] Oral statement of James Miller before the House Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, on Budget Request For U.S. Cyber Command. H.A.S.C. No. 112–26. Washington, D.C., March 16, 2011. – URL: https://www.fas.org/irp/congress/2011_hr/cybercom.pdf

[46] Nakashima, Ellen (2011). NSA allies with Internet carriers to thwart cyber attacks against defense firms. The Washington Post, June 16, 2011. – URL: http://www.washingtonpost.com/national/major-internet-service-providers-cooperating-with-nsa-on-monitoring-traffic/2011/06/07/AG2dukXH_story.html

[47] DHS (2012). Privacy Impact Assessment for the National Cyber Security Division Joint Cybersecurity Services Pilot (JCSP).January 13, 2012. – URL: http://www.dhs.gov/xlibrary/assets/privacy/privacy_nppd_jcsp_pia.pdf

[48] Fryer-Biggs, Zachary (2012). Cyber Sharing Program Formally Expanded. DefenseNews, May 11, 2012. – UIRL: http://www.defensenews.com/article/20120511/DEFREG02/305110001/Cyber-Sharing-Program-Formally-Expanded

[49] DoD (2012). DIB Enhanced Cybersecurity Services (DECS) Procedures. – URL: http://www.dc3.mil/dcise/DIB%20Enhanced%20Cybersecurity%20Services%20Procedures.pdf

DECS, but encouraged them to do so.[50] At the beginning of the new JSCP, emphasis was put on the DIB companies already participating in the CS/IA program[51], but the purpose of program was to broaden the protection to critical infrastructure.[52]

In February 2013, the White House issued executive order 13636 "Improving Critical Infrastructure Cybersecurity" and Presidential Policy Directive 21 "Critical Infrastructure Security and Resilience", effectively extending the program to all operators and owners of critical infrastructure and, once again, renaming the program. The program was now called "Enhanced Cybersecurity Services (ECS)."[53] DHS will provide the same threat indicators with approved private Internet service providers that are used to protect civilian federal government networks; these Internet service providers then may enter contractual relations with providers of critical infrastructure.[54] Defense contractors Lockheed Martin,[55] Raytheon,[56] Northrop Grumman[57], and SAIC[58] joined ranks with AT&T and CenturyLink as approved commercial service providers (CSPs) offering ECS to critical infrastructure operators. DHS uncovered plans that threat indicators will include classified software vulnerabilities, so called zero day exploits.[59] For ECS participants this would increase their protection in an area that would have been extremely difficult to protect otherwise. The executive order is also seen as a reply to the failure of the controversial Cyber Intelligence Sharing and Protection Act (CISPA, H.R. 3523 and H.R. 624), a bill intended to foster sharing of cyber threat information between the government and private companies.

[50] DoD (2012). Defense Industrial Base Cyber Security. Memorandum, October 31, 2012. – URL: http://www.acq.osd.mil/dpap/policy/policyvault/OSD012537-12-RES.pdf

[51] DoD Cybersecurity/Information Assurance (CS/IA) program, URL: http://dibnet.dod.mil

[52] DHS (2012). Privacy Impact Assessment Update for the Joint Cybersecurity Services Program (JCSP), Defense Industrial Base (DIB) –Enhanced Cybersecurity Services (DECS). July 18, 2012. – URL: http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-update-nppd-jcps.pdf

[53] The White House (2013). Executive Order - Improving Critical Infrastructure Cybersecurity. February 12, 2013. – URL: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity; and DHS (2013). Privacy Impact Assessment for the Enhanced Cybersecurity Services (ECS). January 16, 2013. – URL: http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf

[54] Statement of DHS Secretary Janet Napolitano before the U.S. Senate Join Hearing before Committee on Commerce, Science, and Transportation and Committee on Homeland Security and Governmental Affairs on "The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting Our National and Economic Security", March 7, 2013. – URL: http://www.dhs.gov/news/2013/03/07/written-testimony-dhs-secretary-janet-napolitano-senate-committee-homeland-security

[55] Lockheed Martin (2013). Lockheed Martin Named as a Commercial Cyber Security Provider by Dept. of Homeland Security. Media release, February 28, 2013. - http://www.lockheedmartin.com/us/news/press-releases/2013/february/isgs-dhs-cyber-0228.html

[56] Raytheon (2013). Raytheon collaborates with DHS to bolster cyber resiliency for nation's most critical infrastructure. Media release, March 1, 2013. - URL: http://investor.raytheon.com/phoenix.zhtml?c=84193&p=irol-newsArticle&id=1791437

[57] Northrop Grumman (2013). Northrop Grumman Joins Department of Homeland Security Program to Bolster Cyber Protections for U.S. Critical Infrastructure. Media release, May 13, 2013. – URL: http://investor.northropgrumman.com/phoenix.zhtml?c=112386&p=irol-newsArticle&ID=1818734

[58] SAIC (2013). SAIC Signs Agreement With Department of Homeland Security To Be A Commercial Service Provider. Media release, May 15, 2013. – URL: http://investors.saic.com/phoenix.zhtml?c=193857&p=RssLanding&cat=news&id=1820622

[59] Menn, J. (2013). U.S. to protect private sector from software attacks. Reuters, May 15, 2013. – URL: http://www.reuters.com/article/2013/05/15/us-cyber-summit-flaws-idUSBRE94E11B20130515

The executive order comes after a decade of legislative efforts; while legislative proposals were plenty, since FISMA in 2002 no major legislation has been passed that addresses cybersecurity specifically. The executive order does not grant expansive powers nor legal immunity to private companies, however, the Department of Justice has quietly issues so called 2511 letters to telecommunication companies in the ECS program, providing them legal immunity from violations under the U.S. Wiretap Act.[60] This policy and its technological consequences constitute a fundamental shift that institutionalizes how the U.S. government and private companies share cyber threat information and consequently how these networks are protected.[61] Adoption of the ECS program could become mandatory for companies that are regulated by federal agencies with responsibilities towards securing critical infrastructure; this might include companies in specific sectors, such as the defense, health, transportation, chemical and food industry.[62]

5 Discussion

This discussion section will briefly review the development of the Einstein and the ECS program with regards to organizational changes and further the discussion on related transaction costs. Table 2 provides a summary of the two different programs and their iterations.

Table 2 Overview Einstein and ECS Program

Networks	Program Phase	Development Started	Deployment Launched	Description
USG Federal Civilian Networks	Einstein 1	2003	2005	(Block 1.0) Network Flow Information ("NetFlow"), including centralized data storage.
	Einstein 2	2008	2008	(Block 2.0)Intrusion Detection System, to assess network traffic for malicious activities; (Block 2.1) Security Incident and Event Management (SIEM), to enable data aggregation, correlation, and visualization; (Block 2.2) to augment threat information visualization and to provide mechanism for information sharing and collaboration
	Einstein 3	2010	2012	(Block 3.0) Intrusion Prevention System
Private Sector Networks	Enhanced Cyber-security Services (ECS)	2011	2013	ECS was originally introduced by the DoD as the DIB Opt-in Pilot that was handed over in 2012 to DHS as Joint Cybersecurity Services Pilot (JCSP) and evolved into the Joint Cybersecurity Services Program" (JSCP), the DIB Enhanced Cybersecurity Services (DECS), and most recently the Enhanced Cybersecurity Services (ECS). ECS has Einstein 3-like capabilities.

[60] EPIC (2013). EPIC FOIA Request Reveals Details About Government Cybersecurity Program. Electronic Privacy Information Center, April 24, 2013. – URL: http://epic.org/2013/04/epic-foia-request-reveals-deta.html

[61] The executive order includes critical infrastructure providers and all private and public companies that "transport information electronically."

[62] Perera, David (2013). Cybersecurity framework could be mandatory for some companies. FiecreGovernmentIT, February 14, 2013. – URL: http://www.fiercegovernmentit.com/story/cybersecurity-framework-could-be-mandatory-some-companies/2013-02-14

The provisioning of secure Internet access, first for USG networks and later for DIB companies and private operators for critical infrastructure (CI), can be conceptualized as five components of a bundle of products and services. It includes: 1) transport (i.e. connectivity to the rest of the internet); 2) devices and applications; 3) gateway management and configuration (firewalls, security, identity); and 4) information about threats and anomalies. The sourcing of the components of this bundle reflect organizational changes and the expansion of cybersecurity. Table 3 tabulates these components and categorizes for each phase whether or not they are *in-sourced* (IN), out-sourced (OUT), mixed (MIX) or projected (PROJ); also the changes are briefly described. By 'projected' we mean that the federal government extended supply, standards or requirements *to* the private sector.

Table 3 Changes in pattern of secure Internet access production for government agencies

	Pre-Einstein	Einstein 1	Einstein 2	Einstein 3	ECS	
Networks	USG Networks				Private Networks	
Boundaries	within USG			blurred, extended		
Components	**Source**					**Changes**
Transport	OUT	OUT	OUT	OUT	--	From agency level autonomy to TICAP requirements for USG networks and accreditation for CSPs.
Devices and applications	OUT	OUT	OUT	OUT	--	Agency level decisions within FISMA standards; OMB audits for USG networks. Separate norms for CI.
Gateway management and configuration	MIX	MIX	IN	IN	PROJ	From variation across agencies, to agency level decisions within FISMA standards; OMB audits, to TIC program. Separate norms for CI.
Information about threats and anomalies	MIX	IN	IN	PROJ	PROJ	From ad hoc sharing across agencies to US-CERT as coordinator for information sharing to mandatory use of E2 for USG networks. Voluntary for DIB and CI.

5.1 Transaction Costs Considerations

While the federal government never attempted to extend its control or management to Internet connectivity (transport) or to devices and applications, it established firmer hierarchical control over the gateways between federal networks and the public internet, which made it easier and more efficient to implement IDS/IPS throughout the federal government. After the high initial set-up costs of these programs, transaction costs to interface with private sector internet services probably declined, as IDS/IPS came integrated in standardized access services from various commercial Internet service providers. Thus, switching costs or lock-in effects stemming from those managed, outsourced cybersecurity services may be lower than earlier literature on this topic would suggest.

After establishing this capability for federal networks, and sometimes in parallel with the Einstein program, the military and defense agencies moved to project its gateway management and signature production and scanning capabilities into private sector networks. Some of the more ambitious thrusts in this direction (e.g., Perfect Citizen) were blunted by public pressure but ISPs serving government agencies and defense industry firms gain access to classified and unclassified cyber threat information provided by US-CERT and compiled by the U.S. intelligence community.

6 Conclusion

This paper examined how deep packet inspection capabilities in the form of intrusion detection and prevention systems were deployed in U.S. government networks. Co-evolving with this technology development and deployment were various cybersecurity and national security policies. As part of the Comprehensive National Cybersecurity Initiative (CNCI), the U.S. government decided to monitor its federal civilian networks with IDS/IPS capabilities. These capabilities were advanced and extended into private networks via commercial Internet service providers. The NSA and DHS as points of contact provided approved Internet service providers with unclassified and classified cyber threat indicators and signatures to protect federal government networks, DoD defense contractors and operators of critical infrastructure.

Over several phases from 2003 to 2013, responsibilities and organizational boundaries were reassigned and negotiated among different actors. Negotiations focused on the following points: Where would the DPI equipment be located; who would be responsible for operating it; how would it interact with prior security measures; how would compliance with privacy laws be taken into account; how are cybersecurity risks distributed; and how is the control over the new cybersecurity capabilities assigned; what would be classified and what would be open?

The initial steps of the IDS/IPS implementation involved consolidating the federal government's Internet access points and asserting stronger and more centralized control over each agency's arrangements. As the Einstein program went through three different phases, the DPI technology required greater coordination and some degree of organizational centralization. Responsibilities for monitoring and responding to threats are reassigned from individual government and private entities to an intermediary entity, the US-CERT. This equates to a shift from cybersecurity self-production to a more coordinated and consolidated responsibility for US-CERT, which takes a central role in the exchange of information from all levels of government, industry, academia and international partners. It releases alerts about cyber threats and attacks, but also become the central point of contact for the deployment of Einstein. The relationships between DHS, the military agencies and the intelligence community were progressively restructured in ways that changed the relationship between ISPs and government agencies. As the program progressed, the capabilities were continuously extended to include private Internet service providers, state government networks, defense contractors and finally private sector operators of critical infrastructure.

This proved to be politically sensitive and generated pushback from civil society and the private sector. In particular, due to privacy and surveillance concerns the civilian agency DHS had to serve as the 'trusted intermediary' between the private sector actors and the other government agencies, especially the military and intelligence-oriented ones. The ISPs retained control of the DPI equipment but were given signatures by the military and civilian agencies.

The key site of tension and negotiation was the supply of the threat signatures and the situation of the signature monitoring capabilities. In the last phase we saw those capabilities go from being internalized by the federal government and detached from the private sector, to being placed in the private sector network operators' infrastructure but controlled by the government, to being delegated to the private sector actors while making use of some government-supplied signatures, both classified and unclassified.

In this paper, we argue that these policy changes are fundamental, leading to greater interdependence among federal agencies and between federal government and privately-supplied infrastructure. The effects of this extension are observable on several independent levels: the scope of monitored networks; the scope of technological capabilities that determines what can(not) be monitored; a shift from direct monitoring of networks to an indirect, delegated monitoring through commercial Internet service providers; and a switch from voluntary participation to mandatory requirements of such programs. Establishing norms in the form of technology deployments, formal organizational agreements, presidential directives and executive orders and pending cybersecurity legislation are manifestations of the institutionalization of cybersecurity practices.

Depending on one's view, when government agencies seize control over cybersecurity in privately owned Internet and other critical infrastructure, the shifting of boundaries comes with certain benefits or costs. Risk and control are redistributed; some would argue that this reallocation is unilateral. Given the different risk profiles from the military/intelligence, civilian government and private sector but just one infrastructure, securitization of one area affects other interdependent areas accordingly. While the U.S. military/intelligence saw the early Einstein 3 pilots as a model of something bigger, extendable to critical infrastructure, opponents pointed out a narrow path between protecting networks and gathering intelligence information while monitoring them.

References

Auster, Richard D., & Silver, Morris (1979). The State as a Firm: Economic forces in political development (Vol. 3). The Hague: Martinus Nijhoff.

Bellovin, Steve, Bradner, Scott O., Diffie, Whitfield, Landau, Susan, & Rexford, Jennifer (2011). Can it really work? Problems with extending Einstein 3 to Critical Infrastructure. Harvard National Security Journal, 3(1), 1-38.

Bellovin, Steven M., Blaze, Matthew A., Diffee, Whitefield, Landau, Susan, Neumann, Peter G., & Rexford, Jennifer (2008). Risking Communications Security: Potential Hazards of the Protect America Act. IEEE Security and Privacy, 6(1), 24-33.

Brenner, Joel (2011). America the Vulnerable. Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare. The Penguin Press, New York.

Demchak, Chris C. & Dombrowski, Peter (2011). Rise of a Cybered Westphalian Age. Strategic Studies Quarterly, Spring 2011.

Ding, Wen, & Yurcik, William (2005). Outsourcing Internet Security: The Effect of Transaction Costs on Managed Service Providers. Presented at the International Conference on Telecommunication Systems - Modeling and Analysis, Dallas, TX, November 17-20.

Dunn Cavelty, Myriam (2008). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. Routledge.

Eisenhardt, Kathleen M. (1989). Building Theories from Case Study Research. The Academy of Management Review, 14(4), 532–550.

Forte, Francesco (2010). Principles of public economics: a public choice approach. Cheltenham ; Northampton, MA: Edward Elgar.

Goldsmith, Jack, & Wu, Tim (2006) Who Controls the Internet?: Illusions of a Borderless World. Oxford University Press.

Harknett, Richard J. & Stever, James A. (2011). The New Policy World of Cybersecurity. Public Administration Review, May/June 2011, 455-460.

Jensen, Paul H. & Stonecash, Robin E. (2004). The Efficiency of Public Sector Outsourcing Contracts: A Literature Review (November 2004). Melbourne Institute Working Paper No. 29/04. Available at http://dx.doi.org/10.2139/ssrn.625461

Kettl, Donald F. (2000). The Global Public Management Revolution: A Report on the Transformation of Governance, Brookings Institution Press: Washington DC.

Klein, Mark (2009). Wiring Up The Big Brother Machine...And Fighting It. BookSurge Publishing.

Kuehn, Andreas, & Mueller, Milton (2012). Profiling the Profilers: Deep Packet Inspection and Behavioral Advertising in Europe and the United States. Available at http://dx.doi.org/10.2139/ssrn.2014181

Kuerbis, Brenden, & Mueller, Milton (2011). Negotiating a New Governance Hierarchy: An Analysis of the Conflicting Incentives to Secure Internet Routing. Communications & Strategies 81 (1), 125-142.

Landau, Susan (2010). Surveillance or Security? MIT Press.

Mossavar-Rahmani, Shahab (2008). The Protect America Act: One Nation under Surveillance. Loyola of Los Angeles Entertainment Law Review, 29 (1).

Mueller, Milton L., & Asghari, Hadi (2012). Deep packet Inspection and Bandwidth Management: Battles over BitTorrent in Canada and the United States. Telecommunications Policy, 36(6), 462-475.

Mueller, Milton L., Kuehn, Andreas, & Santoso, Stephanie M. (2012). Policing the Network: Using DPI for Copyright Enforcement. Surveillance and Society, 9(4).

Rowe, Brent R. (2007). Will Outsourcing IT Security Lead to a Higher Social Level of Security? Presented at the 2007 Workshop on the Economics of Information Security.

Scharpf, Fritz W. (1997). Games real actors play: Actor-centered institutionalism in policy research. Boulder: Westview Press.

Sourdis, Ioannis (2007). Designs and algorithms for packet and content inspection. Delft: TU Delft.

Warner, Mildred E., & Hefetz, Amir (2012). Insourcing and outsourcing: The dynamics of privatization among U.S. Municipalities 2002-2007. Journal of the American Planning Association, 78 (3), 313-327.

Williamson, Oliver E., & Winter, Sidney G. (1993). The Nature of the firm : origins, evolution, and development. New York, N.Y.: Oxford University Press.

Wolfson, Stephen Manuel (2007-08). The NSA, AT&T, and the Secrets of Room 641A. I/S: A Journal of Law and Policy for the Information Society, 3(3), Winter 2007-08.

Wu, Tim (2010). The Master Switch: The Rise and Fall of Information Empires. Random House.

Yin, R. K. (2008). Case Study Research: Design and Methods (4th ed.). SAGE Publications.

Appendix A: Sample Flow Record

Sample flow record and explanation as provided in DHS Privacy Impact Assessment for Einstein 1.[63]

Sample Flow Record

```
127.0.0.1|192.168.0.20|52119|25|6|10|600|S|2008/04/28T00:02:47.958|44.9
85|2008/04/28T00:03:32.943|SENSOR1|out|S|
sIP|dIP|sPort|dPort|protocol|packets|bytes|flags|sTime|dur|eTime|sensor
|type|initialFlags|
```

Explanation of sample flow record

- 127.0.0.1 (sIP) IP of Computer who is the source of the connection
- 192.168.0.20 (dIP) IP of the computer who is the destination of the connection
- 52119 (sPort) Port the connection was initiated on by the source computer
- 25 (dPort) Port the connection was received on by the destination computer
- 6 (protocol) Protocol number, the number is based on the protocol being used to transport the data (6 = TCP, 1 = ICMP, 17 = UDP)
- 10 (packets) Count of total number of packets seen in this single connection (calculated by the sensor)
- 600 (bytes) Count of total number of bytes seen in this single connection (calculated by the sensor)
- S (flags) Aggregation of all flags seen in this single connection. Flags describe what happened in the connection
- 2008/04/28T00:02:47.958 (sTime) Start time of the connection, Universal Timestamp added by sensor to indicate when the connection was started
- 44.985 (dur) Duration of the connection, this field is calculated (dur = eTime - sTime)
- 2008/04/28T00:03:32.943 (eTime) End time of the connection, Universal Timestamp added by sensor to indicate when the connection was ended
- SENSOR1 (sensor) Name of the Sensor that collected the data, this field is added by the sensor
- out (type) Direction of the traffic (types include “in, inweb, inicmp, out, outweb, outicmp, int2int, ext2ext”)
- S (initialFlags) First flag seen in the connection, this is only based on the first packet of the connection

Flag Markers and their meanings:

- C = CWR - Congestion Window Reduced; E = ECE - Explicit Congestion Notification echo; U = URG – Urgent; A = ACK – Acknowledgement; P = PSH – Push; R = RST – Reset; S = SYN – Synchronize; F = FIN – Finished

[63] DHS (2010). Privacy Impact Assessment Update for the EINSTEIN 1: Michigan Proof of Concept. February 19, 2010. – URL: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_einstein1michigan.pdf

Appendix B: Sample Signature

Sample signature and explanation as provided in DHS Privacy Impact Assessment for Einstein 3.[64]

For illustrative purposes only, the following is an example of a commercially available signature. (This is not a signature the US - CERT intends to use.)

Signature:

```
alert tcp any any -> $HOME_NET 443 (msg: "DoS Attempt";
flow:to_server, established; content:"|16 03 00|"; offset:0; depth:3;
content:"|01|"; within:1; distance:2; byte_jump:1,37,relative,align;
byte_test:2,>,255,0,relative; reference:cve; classtype:attempted-dos;
sid:2000016; rev:5;)
```

Explanation of Signature:

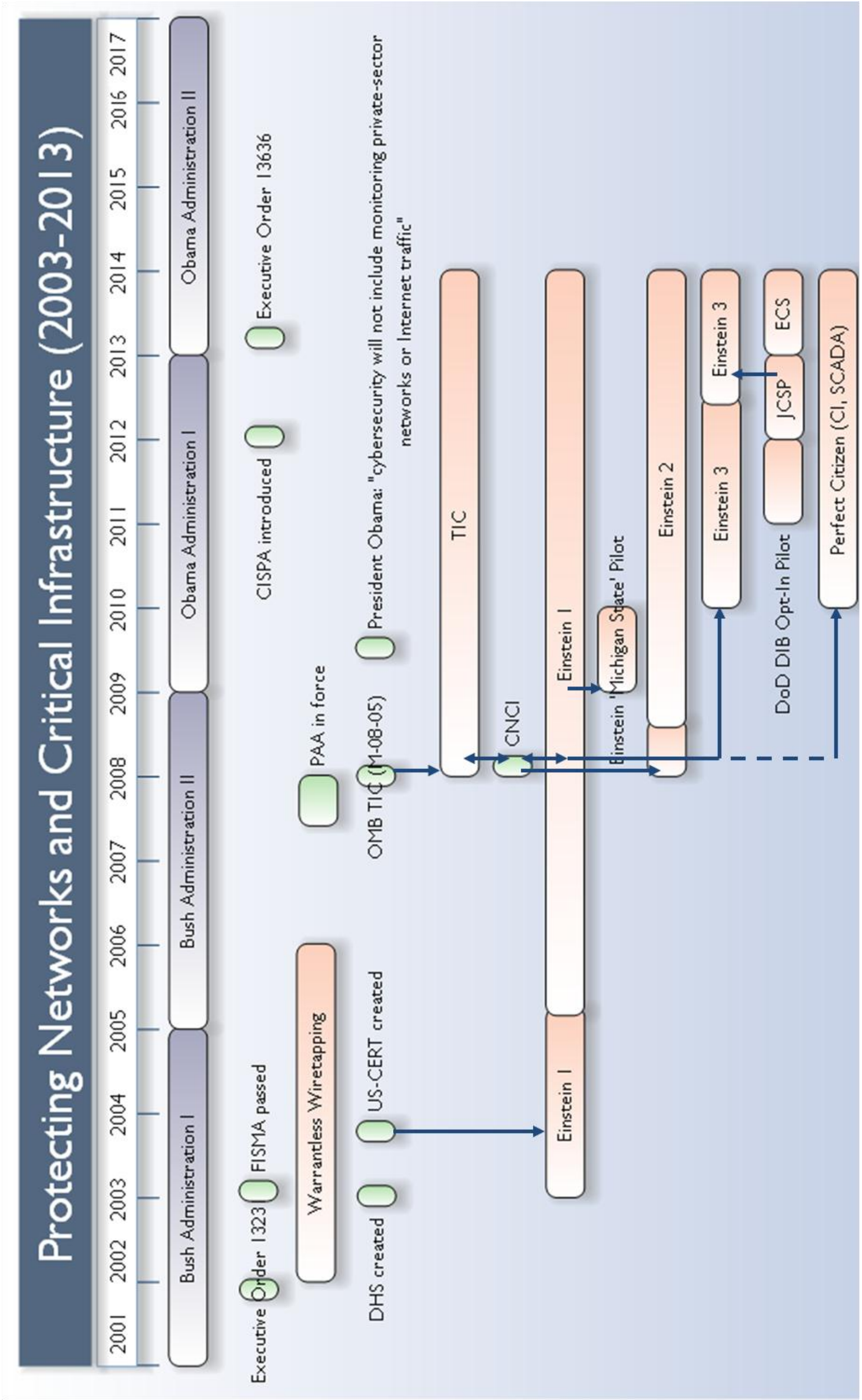
Alert:	Type of IDS Event
tcp:	Protocol being examined
any:	Any source IP
any:	Any source port
->:	Direction (points to @HOME_NET which indicates inbound)
$HOME_NET:	A variable which is defined by the IDS as the subnets that make up the internal network
443:	Destination port traffic is bound for
msg:"DoS Attempt":	Name of the alert that is sent to the console (for humans reading the alert console)

The remaining fields of the string tells the IDS what to look for, the breakdown of the commands and instructs the IDS where in the packet to look for the text.

This signature example tells the IDS to alert on any external IP on any external port that sends traffic to the home network, on port 443, with the text – "|16 03 00|", and the text – "|01|" within certain parameters and offsets. The alert name is defined as – "DoS Attempt" and references CVE, SID:2000016, revision 5.

[64] DHS (2010). Privacy Impact Assessment for the Initiative Three Exercise. March 18, 2010. – URL: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3exercise.pdf

Appendix C: Timeline


Protecting Networks and Critical Infrastructure (2003-2013)
Bush Administration I
Bush Administration II
Obama Administration I
Obama Administration II
Executive Order 1323
FISMA passed
CISPA introduced
Executive Order 13636
Warrantless Wiretapping
PAA in force
DHS created
US-CERT created
OMB TIC (M-08-05)
President Obama: "cybersecurity will not include monitoring private-sector networks or Internet traffic"
TIC
CNCI
Einstein I
Einstein I
Einstein 'Michigan State' Pilot
Einstein 2
Einstein 3
Einstein 3
JCSP
ECS
DoD DIB Opt-In Pilot
Perfect Citizen (CI, SCADA)