Airman maintains communications cabling including copper wiring, indoor and outdoor cabling, and telephone switches (U.S. Air Force/George Goslin)

# Information-Sharing with the Private Sector

By Veronica A. Chinn, Lee T. Furches, and Barian A. Woodward

Imagine logging onto your bank's secure Web site using your personal computer to pay monthly bills or transfer money between accounts to pay your mortgage. When you enter the Web site address or try to access a favorite link, you receive an error message. You check to see if your router is working and then verify that your Internet service is connected. You check other Web sites, and they load without issue. You call your bank to report the problem and they tell you their service should be available as soon as they fix a technical issue. Meanwhile, time is ticking toward the due date on your bills. This is what can happen when a major bank is under a denial-of-service attack.

At PNC, Wells Fargo, J.P. Morgan Chase, Bank of America, and a host of other big-name banks, this problem occurred in September 2012 and again the following January.[1] Millions of customers could not reach their accounts online because so-called hacktivists were using this method of cyber ransom to prove what they were capable of and to make political points.[2] Most major banks have some protection against such attacks.

Lieutenant Colonel Veronica A. Chinn, USA, is a Future Operations Planner at U.S. Cyber Command. Lieutenant Colonel Lee T. Furches, ANG, currently serves as the Air National Guard Strategic Planner in the Office of the Assistant to the Chairman of the Joint Chiefs of Staff for National Guard and Reserve Matters. Major Barian A. Woodward, USMC, currently serves as a Cyber Defense Capabilities Officer with U.S. Strategic Command.

If they require assistance, the Federal Bureau of Investigation (FBI) has developed the capability to track down many criminal organizations involved in denial-of-service attacks. But what if would-be attackers, sponsored by terrorist groups, nonstate actors, or nation-states, organized themselves to conduct a concerted cyber assault of more than the financial sector? That might be more than even the FBI could handle.

Since nongovernmental entities own and operate a large majority of cyberspace and critical infrastructure, the United States needs not only a whole-of-government approach to cybersecurity but also a whole-of-nation approach. The U.S. Government must articulate the details of such an approach in a strategic framework that identifies a significant role for the private sector. To develop that framework, the Nation needs robust information-sharing between government and industry.

In 2003, the Bush administration issued the beginnings of such a strategy with its *National Strategy to Secure Cyberspace* (NSSC), which called for greater linkages between the public and private sectors. Unfortunately, over the past decade, several shortfalls or ill-conceived initiatives prevented the establishment and maturation of such cooperative paradigms. To engender a whole-of-nation approach to cybersecurity, the U.S. Government must tailor legislative and executive branch efforts to cybersecurity, enable information flow between the Intelligence Community (IC) and the industrial sector, address overclassification of threat reporting information, and maintain assignment for the national lead in cybersecurity to an entity outside the IC.

The NSSC was the first foundational strategic guidance document produced by the United States focused exclusively on cybersecurity. The strategy centers on five mutually supporting priorities:

- National Cyberspace Security Response System
- National Cyberspace Security Threat and Vulnerability Reduction Program
- National Cyberspace Security Awareness and Training Program
- Securing Governments' Cyberspace
- National Security and International Cyberspace Security Cooperation.[3]

A key concept presented in the strategy is "public-private partnership." President George W. Bush stated, "Reducing . . . [cybersecurity] risk requires an unprecedented, active partnership among diverse components of our country and our global partners."[4] This statement suggests that national leadership at the highest level recognized the need to engage outside the government apparatus over a decade ago. The executive branch released the draft version of the strategy to the public for review and convened 10 town hall meetings across the country to elicit feedback. The public was considered an integral part of the resulting strategy.[5]

The NSSC prescribes a whole-of-nation approach and accordingly provides a baseline for analysis of national efforts to secure cyberspace. Its priorities are separate and distinct, each with its unique required actions and initiatives, but a common requirement is information-sharing. In subsequent years, there were numerous reasons for the government's inability to fully develop a culture of information-sharing between the public and private sectors, but four issues stand out.

## Information-Sharing Impediments and Shortfalls

First, executive and legislative branch efforts intended to address information-sharing in our post-9/11 reality failed to emphasize all-threat cybersecurity. Rather, most of these narrowly scoped undertakings focused exclusively on counterterrorism. For example, the President issued the *National Strategy for Information Sharing* and Executive Order (EO) 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans.* Both apply exclusively to combatting terrorism. Congressional efforts as well, to include the comprehensive Intelligence Reform and Terrorism Prevention Act of 2004, focused solely on counterterrorism. Certainly all these efforts can provide value in countering terrorist-originated cyber attacks. However, defending the Nation against cyber threats transcends such a single-threaded, counterterrorism-steeped scope.

National cybersecurity is an ambitious, broadly focused endeavor seeking to counter a wide spectrum of threats, which certainly encompasses terrorist-launched cyber attacks. However, the cyber threat spectrum includes many nonterrorist dangers as well. The teenaged "script kiddie" in his mother's basement, who may be a cliché but is not yet passé, still presents a risk to national infrastructure. Highly organized cyber criminals hack into and mine financial companies' databases for monetary gain. Internet-based activists—or hacktivists—illegally access computer systems to draw attention to their politically or socially motivated causes. And powerful nation-states back increasingly robust cyber espionage programs. With such a myriad of threat actors and motivations, the United States cannot rely exclusively on counterterrorism-focused intelligence reform as a proxy for broader reforms optimized for the unique pursuit of all-threat cybersecurity.

Second, the IC has few mechanisms for the seamless flow of information to and from potential industry partners. The ideal role for both the public and private sectors involves information-sharing and flow in both directions. For example, industry must share its real-time observations about cyber attacks with the government on its networks so agencies can warn other companies about these threats. Also, the government, particularly the IC, must be willing and enabled to share its threat reporting information with the private sector. The Nation's critical infrastructure owners and operators will then be better able to secure their systems. At present, information-sharing does not occur optimally in either direction. Private industry currently sees two main disincentives to information-sharing with the government. Their primary concern is privacy. These companies are generally concerned that information

they share about intrusions into their networks may leak to competitors or potential customers and negatively impact their bottom lines. Also, they fear liability, especially if it becomes known that they lost data or caused the loss of data critical to another company's or individual's financial well-being. These issues significantly impede reporting of cyber attacks to the government.

For its part, the Intelligence Community unfortunately focuses almost exclusively on information-sharing among its 17 member agencies and organizations. To its credit, the IC seems to understand the need for a broader information-sharing focus. While the White House and Congress concentrated rather myopically on terrorism, the IC developed more broadly focused publications. Specifically, their 2008 information-sharing strategy and 2009 Intelligence Community Directive Number 501 implement 2004 intelligence reform act imperatives. These documents are not counterterrorism-specific, which allows potential for their broad application. However, their shortfall in the context of nationwide information-sharing is that they do not facilitate sharing outside the IC. As observed, many other entities—from state and local governments to non-IC military organizations to private industry—have a significant stake and role in the national solution to cybersecurity.

Due to the extreme sensitivity of its work, the Intelligence Community has an institutional but understandable reluctance to share information. However, cybersecurity differs from most IC missions in its inextricable relationship to the industrial base. The need for information-sharing in this arena is similar to that recognized over the past decade in counterterrorism. The government must now extend the lessons learned in counterterrorism information-sharing to cybersecurity. In 2011 congressional testimony, Zoë Baird Budinger and Jeffrey H. Smith of the Markle Foundation observed, "This transformation we are seeing in counterterrorism is built upon principles and practices that can be extended to other key homeland security priorities so that our government can work in a more modern, decentralized, public-private manner to address growing challenges like cybersecurity and economic security."[6]

A key element of extending such an information-sharing paradigm expressly to cybersecurity will include sharing related threat-reporting information. The IC holds much of this information in its databases. Unfortunately, the classification of this information often limits its dissemination to many who could use it to enhance the Nation's cybersecurity. This leads us to a related impediment to information-sharing.

Third, the tendency toward overclassification of relevant data impedes the flow of useful information to industry partners. Setting the stage for the discussion following the 2001 terrorist attacks, *The 9/11 Commission Report* concluded:

*Current security requirements nurture over-classification and excessive compartmentalization of information among agencies. Each agency's incentive structure opposes sharing, with risks (criminal, civil, and internal administrative sanctions) but few rewards for sharing information. No one has to pay the long-term costs of over-classifying information, though these costs—even in literal financial terms—are substantial. There are no punishments for not sharing information. Agencies uphold a "need-to-know" culture of information protection rather than promoting a "need-to-share" culture of integration.*[7]

Pursuant to specific 9/11 Commission recommendations and complementary to the Intelligence Reform and Terrorism Prevention Act of 2004, Congress passed the Reducing Over-Classification Act in 2010.[8] Most significantly, the act requires inspectors general from all Federal departments or agencies with original classification authority to conduct a review of classification policies and identify those that may contribute to misclassification of information.[9] Per a 2011 Department of Defense (DOD) Inspector General memorandum, this review is ongoing.[10]

If the DOD review includes the National Security Agency (NSA), arguably the most prolific generator of cybersecurity threat reporting, this act could improve the quantity and usefulness of cybersecurity threat reporting available for sharing among Federal, state, and local governments and private industry. Until this review is complete, however, the Federal Government must remain cautious about overcommitting the work of cybersecurity to the extremely capable but super-secretive agency, bringing us to our final issue: the United States must resist the urge to transfer primary responsibility for national cybersecurity to NSA.

The NSA has remarkable experience in cyberspace operations and information assurance in the DOD realm, but while its preeminent expertise is immensely useful in nonmilitary cybersecurity issues, assigning the lead to NSA would almost certainly prove counterproductive in fostering whole-of-nation collaboration. To illustrate the fears this proposition instills in the cybersecurity community, we can examine the reaction to comments from then Director of National Intelligence Dennis Blair. In congressional testimony in 2009, he kicked off a firestorm within the Department of Homeland Security (DHS) and the private sector by suggesting that NSA's extensive cybersecurity expertise should be "harnessed" to secure Federal and critical infrastructure networks.[11] Many saw this as a play for a lead role in national cybersecurity and expressed concern that NSA would gratuitously enshroud its cybersecurity efforts under high levels of classification. Such a transfer of responsibility would make whole-of-nation collaboration on cybersecurity difficult or even impossible.

The 2008 *Comprehensive National Cybersecurity Initiative* (CNCI) stands as a related example of the effect an overly secretive approach might have on collaboration. Blair testified that the CNCI "develops a framework for creating in partnership with the private sector an environment that no longer favors cyber intruders over defenders."[12] However, the CNCI is classified Secret. Many question how a classified initiative can support

Airman uses spectrum analyzer to check television broadcast network routers (U.S. Air Force/Val Gempis)

such collaboration with the private sector if that community cannot even access the plan. The lead for cybersecurity is best left in the hands of an organization less prone to overclassification of its work. In 2003, NSSC assigned DHS as the lead, and so it should remain, with augmentation from NSA and other agencies.

## Recent Executive Actions

Many argue that EO 13636, *Improving Critical Infrastructure Cybersecurity*, and Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience*, take the next step toward creating the whole-of-nation approach envisioned by the NSSC. Both documents focus on critical infrastructure due to the impact on national security, economic stability, and public safety that could result from a deliberate cyber attack. They only differ in their approach. Taken together, they make progress toward a whole-of-nation effort but only constitute a partial solution in the end.

According to Harold Relyea, a specialist in American National Government at the Congressional Research Service and author of the report *Presidential Directives*, there are two primary differences between an executive order and a Presidential policy directive. An executive order has a statutory requirement to be published in the *Federal Register*, but a PPD has no such requirement, which means a PPD can be classified. Additionally, an executive order must be circulated to a general counsel or similar agency attorney as "a matter of circulation and accountability."[13] These differences aside, an opinion written by the Justice Department Office of Legal Counsel in 2000 concludes that "executive orders and directives are equivalent in their force and impact."[14]

EO 13636 directs three primary tasks that must be initiated to set conditions for further improvement of cybersecurity. The first is to identify the critical infrastructure at greatest risk to cyber attack based on the current threat, its vulnerability to cyber attack, and the impact on national interests of its degradation or destruction. The second is to improve information-sharing and ways to more effectively produce, disseminate, and track classified reports that involve critical infrastructure owners and operators. The third is the establishment of a "Cyber Security Framework." The order sets a 2-year timeline to accomplish all these actions with the majority of them within 120 days of the order's publication.[15] Each of these tasks identifies DHS as the lead agency with other agencies in support.

In the words of Frederick the Great, "He who defends everything defends nothing." This is no less true in cyberspace than in other forms of warfare, given the tremendous expansion of Internet infrastructure over the past two

May 2013 workshop to facilitate discussions on work carried out in area of cyber security under Action Line C5 (ITU/Claudio Montesano Casillas)

decades. Therefore, the United States must prioritize the most critical facilities or systems that comprise the backbone of our societal functions. EO 13636 required DHS to provide the initial prioritization of those critical infrastructure facilities at greatest risk to cyber attack by July 2013. The prioritization uses a risk-based approach to examine how a cybersecurity incident could reasonably result in a catastrophic regional or national effect on public health or safety, economic security, or national security. Heads of Sector Specific Agencies (SSAs) must be involved in the process and facilitate information exchange and recommendations from the private sector.

Regarding information-sharing, the executive order takes a two-pronged approach in improving accessibility of cyber threat information to critical infrastructure owners and operators. One approach is deliberately producing unclassified reports to the greatest extent possible. The second calls for granting security clearances and classified access to accommodate instances in which a report cannot be declassified but the information is crucial to the defense of critical infrastructure. While this task addresses access, the matter of identifying what information is to be shared is a subtask of the Cyber Security Framework.

Also, as part of EO 13636, the National Institute for Standards and Technology (NIST) was tasked to implement its final version of a Cyber Security Framework by February 2014. The executive order defines the Cyber Security Framework as "a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."[16] The EO describes what the framework will provide as "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk."[17] In military terms, it might be considered a standard operating procedure, a guide against which critical infrastructure companies measure themselves to ensure they instituted the most sensible and secure measures to protect their networked systems from cyber attack.

The Information Technology Laboratory, a branch under NIST, has undertaken the Cyber Security Framework project. The laboratory has "the broad mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology through research and development in information technology, mathematics, and statistics."[18] In the Cyber Security Framework, the laboratory now has an immensely challenging task that will entail interfacing with many entities, both public and private.

Similarly, PPD-21 directs a set of tasks that support the NSSC and requires agencies across the government, as well as industry, to provide input towards a potential solution.[19] The directive reinforces the 2003 strategy, which suggests that in order to secure U.S. interests in cyberspace, we must ensure that our networks are both protected and resilient. More specifically, it complements the edicts issued in EO 13636 with additional directives seeking to define both the public and private sector cyber environments to establish better starting points for a national movement toward greater cybersecurity.[20] So while EO 13636 focuses on the critical tasks, PPD-21 focuses on the supporting tasks.

PPD-21 introduces three strategic imperatives that will support and enable the original objectives in the 2003 NSSC: refining and clarifying functional relationships across the Federal Government, enabling information exchange through establishing a baseline for data and system requirements, and information integration and analysis streamlined to inform planning and operational decisions.[21] These imperatives provide the foundation on which the specified tasks in both EO 13636 and PPD-21 can build.

Each task specified in PPD-21 requires DHS to take the lead either solely or in cooperation with SSAs.[22] The first task is to describe the functional relationships across government agencies. This is essentially a comprehensive "who does what" effort at the intersection of critical infrastructure and cyberspace. This may take the form of a basic point-of-contact list, which constitutes a starting point for coordination. The second task is to evaluate existing public-private information-sharing models and recommend what needs to be sustained or changed. The third task is identification of baseline data and system requirements that should serve as the minimum standard for cybersecurity. Fourth, by October 2013, DHS

was to provide a demonstration of a near real-time situational awareness capability for critical infrastructure threats and vulnerability assessment. Fifth, DHS must produce a document that will supersede the *National Infrastructure Protection Plan* of 2009. The final requirement is a research and development plan specific to critical infrastructure security and resilience. This plan is due 2 years from the PPD date of publication.[23] DHS has already been working on many of these tasks as part of existing efforts. However, the PPD creates a temporal constraint to emphasize the urgency and necessity of the six tasks.

## Remaining Gaps and Potential Legislative Solutions

EO 13636 and PPD-21 in many ways effectively focus on information exchange, along with the critical requirement for resolving the observed impediments and shortfalls and implementing the NSSC information-sharing intent. While these directives provide a workable way ahead in many areas, they are not without significant challenges.

Regarding the first impediment to information-sharing—exclusive focus on counterterrorism with some inattention to cybersecurity—the executive order and PPD represent a refreshing change of direction. These documents demonstrate a concerted effort on the part of the Obama administration to develop much-needed guidance and policy that are specific to all-threat cybersecurity. Of course, these executive branch directives cannot address legislative shortcomings in this regard.

Some bills are circulating through Congress, most notably H.R. 3523, the Cyber Intelligence and Sharing and Protection Act (CISPA). If passed, this act would reiterate many elements already included in EO 13636. Additionally, the bill has potential to address other shortfalls the executive order could not cover due to separation-of-powers issues.

Given current budgetary constraints, one potential element of legislation may be resourcing for EO 13636–related efforts. For example, the executive order directly tasks DHS with expediting security clearance processes, which the department should be able to resource within its current budget authority. However, the order does not provide the resources to extend classified data networks to the critical infrastructure owner and operator's facility or to provide physical security at the new classified material handling location. As Congress holds the "power of the purse," complementary legislation can support the executive order in this and other concerns.

For information-sharing between the IC and industry, the executive order largely addresses the flow in one direction—from the government to private industry. CISPA or other legislation would need to address the flow in the opposite direction. The legislation could potentially include legal standards for government personnel handling sensitive information that pertains to private industry's cyber-based intrusions. Legislators would also need to address liability concerns and further incentives for industry participation in the executive order's voluntary programs. For example, expansion of the Enhanced Cyber Security Services Program bolsters the public-private partnership; however, being a voluntary program means that private industry participation is uncertain at best. The Cyber Security Framework, in varying degrees, builds on NSSC priorities, but its success is also tied to voluntary participation. One of several deterrents to private industry participation may be companies' concern for business confidentiality. Without supporting legislation, EO 13636 lacks the resources to offer incentives to increase participation or—as a last resort—compel participation by law. The program must address the concerns of private industry one way or another to improve participation.

For the flow of information from the government to the private sector, overclassification will likely linger as an impediment to truly useful information exchange. EO 13636 directs the greatest possible development of unclassified reports of cyber threats that identify "a specific targeted entity."[24] This is a positive step toward improving the cybersecurity of U.S. critical infrastructure. Unfortunately, the overclassification of data feeding these reports could compromise the integrity of this goal.

To develop unclassified reports, U.S. agencies must strip out any information that suggests the presence of an intelligence source. Such data are routinely classified at the Top Secret, Secure Compartmented Information (SCI) level. The more SCI data there are in the original report, the less likely it is that a redacted report would be possible or useful. Thus, Congress must take action on the issue of overclassification of cybersecurity threat reporting. Legislators could address gratuitous classification through new acts such as CISPA or through cyber-specific modifications of existing legislation, particularly the Reducing Over-Classification Act.

Many will point out that too much information-sharing can prove catastrophic to national security. A commentary from the Central Intelligence Agency Center for the Study of Intelligence laments the nascent information-sharing paradigm and observes, "the newly enshrined emphasis on 'need to share' has swung the pendulum much too far in the opposite direction."[25] Certainly the 2010 WikiLeaks scandal is an example of vulnerabilities to sensitive information. U.S. Army Private First Class Bradley Manning allegedly provided over 260,000 diplomatic cables, over 90,000 intelligence reports, and one video to the WikiLeaks site, which is dedicated to transparency of government.[26] While most of the information was classified, none of the compromised information exceeded the Secret level, presumably because PFC Manning only had routine access to Secret-level networks. In this case, a downgrade of Top Secret information to Secret or lower could have subjected even more information to compromise on WikiLeaks.

While some may see WikiLeaks as a reason to increase security of sensitive information and reduce sharing, prudent policymaking will consider the dangers of such a potentially overreactive policy. While we must secure our classified information, national security as extended

into cyberspace still depends on the flow of information among all parties who can contribute to our collective defense. Thus we must strike a balance between the need for information security and sharing. Accordingly, policymakers should view WikiLeaks as a reason for developing and refining policies, procedures, and constructs for monitoring and tracking information while ensuring its provision to those who may find it useful for their national security work.

Another effort to address classified information flow is to increase the number of private entities that have access to classified cyber threat information. The expansion of the Enhanced Cyber Security Services Program will enable this effort and include critical infrastructure companies and commercial services providers. In its current state, the program provides cyber threat information as well as mitigation standards and procedures to defense industrial base companies. To mitigate issues associated with classified information elsewhere in the private sector, the executive order calls for expediting the security clearance process of "appropriate personnel employed by the critical infrastructure owners and operators."[27] While EO 13636 makes significant strides in bolstering the government–private industry partnership through these efforts, the effectiveness of the order remains uncertain without legislation in support of the policy.

Concerning the fourth and final impediment to public-private information-sharing, the executive branch used its executive order and PPD to clearly reaffirm DHS as the lead for cybersecurity. This is an appropriate measure toward avoiding concerns about "militarization" of cyberspace. That said, NSA has tremendous expertise in cyberspace situational awareness. Additionally, the Defense Department's unique legislative authorities to conduct offensive actions make it *the* key entity in some responses to external attacks on U.S. critical infrastructure. The executive and legislative branches may therefore need to consider additional measures to facilitate the collaboration among all key entities with a stake in U.S. cybersecurity.

Since the release of the 2003 *National Strategy to Secure Cyberspace*, government efforts to attain prescribed intragovernmental and public-private information-sharing have proved fractured and incomplete. Issues have ranged from a lack of concerted focus on cybersecurity in both the executive and legislative branches, to a lack of information-sharing to and from the Intelligence Community, to a systemic tendency to overclassify cyber threat reporting information, to distracting considerations to center the lead for cybersecurity within the military. The Obama administration's Executive Order 13636 and Presidential Policy Directive 21 made positive steps toward rectifying many shortcomings. However, these actions represent only a part of the solution. Congress now must act to provide complementary cybersecurity legislation to fill gaps in the public-private information-sharing construct prescribed in the 2003 strategy. Only then will the United States be fully on the path to a whole-of-nation approach to meet the full scope of cyber threats. **JFQ**

## Notes

[1] Michael Mimoso, "Bank DDoS [distributed denial-of-service] Attacks Using Compromised Web Servers as Bots," *Threatpost.com*, January 11, 2013, available at <http://threatpost.com/bank-ddos-attacks-using-compromised-web-servers-bots-011113/77393>; Mimoso, "'Historic' DDOS Attacks Against Major U.S. Banks Continue," *Threatpost.com*, September 27, 2012, available at <http://threatpost.com/historic-ddos-attacks-against-major-us-banks-continue-092712/77055>.

[2] Mimoso, "Bank DDoS Attacks."

[3] Department of Homeland Security (DHS), *National Strategy to Secure Cyberspace* (Washington, DC: DHS, February 2003), x.

[4] Ibid., 11.

[5] Ibid., iv.

[6] Zoë Baird Budinger and Jeffrey H. Smith, Statement Before the Senate Committee on Homeland Security and Governmental Affairs, *Ten Years After 9/11: A Status Report On Information Sharing*, October 12, 2011, available at <www.hsgac.senate.gov>.

[7] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, DC: U.S. Government Printing Office, July 22, 2004), 417.

[8] Reducing Over-Classification Act, Public Law 111-258, U.S. Statutes at Large 124 (2010), 2648.

[9] Ibid.

[10] Patricia A. Brannin, memorandum to Secretaries of the Military Departments et al., October 26, 2011, available at <www.fas.org/sgp/othergov/dod/ig-overclass-2011.pdf>.

[11] Dennis C. Blair, Director of National Intelligence, Statement Before the House Permanent Select Committee on Intelligence, Annual Threat Assessment, February 25, 2009.

[12] Ibid.

[13] Steven Aftergood, "What's the Difference Between an Executive Order and a Directive?" *Secrecy News*, February 14, 2013, available at <www.fas.org/blog/secrecy/2013/02/eo_pd.html>.

[14] Ibid.

[15] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013, available at <www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

[16] Ibid.

[17] Ibid.

[18] Information Technology Laboratory, "National Institute of Standards and Technology," available at <www.nist.gov/itl/what-itl-does.cfm>.

[19] Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, February 12, 2013, available at <www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

[20] Executive Order 13636.

[21] Presidential Policy Directive 21.

[22] Ibid.

[23] Ibid.

[24] Executive Order 13636.

[25] Bowman H. Miller, "The Death of Secrecy: Need to Know . . . with Whom to Share," *Studies in Intelligence* 55, no. 3 (Center for the Study of Intelligence November 9, 2011).

[26] "Bradley Manning," *The New York Times*, January 9, 2013, available at <http://topics.nytimes.com/top/reference/timestopics/people/m/bradley_e_manning/index.html>.

[27] Executive Order 13636.