Testimony on Behalf of the Markle Task Force on National Security in the Information Age

US SENATE HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS COMMITTEE

Hearing on Information Sharing in the Era of WikiLeaks:
Balancing Security and Collaboration

MARCH 10, 2011

Mr. Chairman, Senator Collins, thank you for holding this hearing and dedicating your time and energy to the critical issue of information sharing. And thank you for inviting the Markle Task Force on National Security in the Information Age to submit written testimony in order to help inform the current discussion. You have led this effort since the attacks of 9/11 with a singular commitment to making this nation safer. Since 2002, the Markle Task Force has provided policymakers, including this Committee, with recommendations[1] to help accelerate our government's use of information and information technology to better understand the threats we face and make better decisions about those threats. Our ultimate goal has been to help enable the federal, state, and local governments to work together to protect our nation from terrorism and other threats.

A substantial change has occurred throughout government in the way security professionals do business. Information sharing has become more widespread and the government has made some real changes necessary to respond to new threats. That said, progress has been too slow in some places and has lacked adequate guidance or oversight in others. In light of the recent series of releases of sensitive and classified documents, this progress in sharing information between and among government agencies may be reversed. In October—before the most recent release of the Department of State cables—Director of National Intelligence Clapper observed that the release of classified information by WikiLeaks may have a "chilling effect" on information sharing.[2]

We believe that the government must devote serious attention to preventing further leaks. Policies to control access to information in the Information Sharing Environment are not adequately developed and

[1] For more information on all of our previous work on information sharing, please visit www.markle.org/national-security.

[2] Jason Ryan, "President Obama and Intelligence Director Angered Over Media Leaks," *ABCNews,* 6 October 2010, available at http://abcnews.go.com/Politics/president-obama-intelligence-director-angered-media-leaks/story?id=11817252 (last visited 1 March 2010).

inadequate audit tools are in place. The government uses both policy and technology correctly in certain arenas, but for years we have urged stronger action across government, led from the top. Nevertheless, efforts to reduce the sharing of information would be misguided and potentially a risk to our national security. Our government has improved how it operates since 9/11, and this improvement needs to be encouraged and sustained. We agree with the statement you, Senators Lieberman and Collins, made in your recent Wall Street Journal op-ed that "…a return to the pre-9/11 era, when agencies hoarded information, would compromise our national security."[3]

Indeed, efforts to reduce information sharing between and among government agencies and the private sector would not only compromise our national security; these efforts might also reduce the public's confidence in other government information sharing programs such as those necessary for the development of health information exchange and the smart grid. The success of these programs, which promise tremendous cost savings, quality improvements, and efficiency gains, is critical for modernizing government and private sector operations and building the foundation for continued innovation and growth in the information economy.

The Need for Information Sharing

The attacks on 9/11 showed all of us that the Cold War "need to know" system for managing classified and sensitive information drove a culture of information security that resulted in countless stovepipes of information and secretive pockets of the nation's most valuable information. This system did not keep America safe in a world of asymmetric threats. Many realized that protecting America in this new threat environment would require the government to operate in an entirely new way.

You have enacted two major laws that have substantially changed how government understands those who would do us harm and how it acts to prevent that harm. We have tried to contribute to this same challenge. Over the course of four reports written between 2002 and 2009[4], the Markle Task Force grappled with how the government could operate in a new way. With national security experts from every administration since President Carter, civil liberties advocates, information technology executives, academics, and many from within government and the intelligence community, we proposed a collaboration across agencies that would foster a robust sharing of information and ideas. This collaboration, to be successful, required a set of policies that would simultaneously empower and constrain government officials by making clear what collection, analysis, sharing, and uses of information were permissible, and what were not. Instead of storing data centrally, we suggested storing data on a distributed network, thus eliminating the gaps between government agencies and empowering all players in the network—including those at the edges—to create and share actionable and relevant information.

[3] Joseph I Lieberman and Susan M. Collins, "How to Prevent the Next WikiLeaks Dump," *The Wall Street Journal,* 13 January 2011, available at http://online.wsj.com/article/SB10001424052748703779704576074340363346676.html (last accessed 7 March 2011).

[4] All Markle Task Force reports are available at http://www.markle.org/national-security/publications-briefs-national-security.

The objective of this network was to enhance the government's ability to discern indicators of terrorist activity amid overwhelming amounts of information, and to create more time for the nation to respond to threats more effectively.

Since 9/11, there has been a shift in federal and state government culture towards this type of information sharing and collaboration model, and some segments of the government have made progress implementing information sharing policies. Government sources indicate that this approach, in turn, has been very successful. In 2010, for example, the Obama administration claimed twenty-two counter-terrorism successes that resulted, in part, from increased information sharing.[5] These successes included charging fourteen individuals with terrorism violations for providing al Shabab with money, personnel, and services; arresting Farooque Ahmed for plotting to bomb Metrorail stations in the Washington, DC area; and discovering and disarming multiple bombs on cargo planes bound for Chicago. The agility that sharing information has given our government officials has enabled them to better understand our rapidly changing world. If information sharing policies and practices had not been implemented, these recent successes might have been tragedies. Clearly, now is not the time to turn back the clock on information sharing.

Of course, there are risks inherent in sharing more information, but these risks are outweighed by the risks of not sharing. The attacks on 9/11 illustrate a stark example of this.

The Breach

Public sources indicate that the recent information breach to WikiLeaks, allegedly committed by PFC Bradley Manning, apparently occurred primarily because of a lack of appropriate policies and technologies that limit the risks of increased access to sensitive and classified information. PFC Manning described the situation he encountered when he downloaded 1.6 gigabytes of classified US government data onto re-writable compact disks: "Weak servers, weak logging, weak physical security, weak counterintelligence, inattentive signal analysis . . . A perfect storm."[6]

The security breach was not an inevitable result of information sharing. We do not have access to any information other than that which has been published in the media, but it appears that the breach was the result of the lack of adequate controls about access to information.

Instead of reducing information sharing, the government should work to minimize the risk that unauthorized disclosures occur by building government-wide authorities and constraints into all

[5] Prepared Remarks of John Brennan, Director of National Intelligence, to the White House Press Corps, "Fact Sheet on Security Enhancements: Statement by John Brennan on Holiday Security," 22 December 2010.

[6] "Bradley Manning, in his own words: 'This belongs in the public domain,'" *The Guardian*, 1 December 2010, available at http://www.guardian.co.uk/world/2010/dec/01/us-leaks-bradley-manning-logs (last visited 1 March 2011).

information sharing policies and systems. We have counseled greater urgency in this area for many years.[7] As we develop the capability to better share information, we need at the same time to develop the regulations, processes, and use of technology that control access and use.

Authorities and Constraints

Much of the intelligence community and many in other agencies charged with national security have embraced the objective of collaborating across agency lines and sharing more information with those who need it to fulfill their mission. However, the February 2011 GAO report on "high risk" government programs noted, "The government has continued to make progress during the past two years in sharing terrorism-related information among its many security partners, but does not yet have a fully-functioning Information Sharing Environment in place."[8] Implementation of information sharing programs has been uneven across agencies and has not been driven by a government-wide vision of the authorities and constraints necessary to build an effective and trusted information sharing environment.

An essential element of an information sharing environment is that prior to making information available to a wide community, the government should have regulations and processes for controlling access to and use of shared information. Instituting these mechanisms is a critical step in the effort to shift how the government does business. These mechanisms include a standard of authorized use and immutable audit logs. Together, these tools can both prevent unauthorized disclosure of information and help build confidence in the Information Sharing Environment.

Authorized Use[9]

In our third report, *Mobilizing Information to Prevent Terrorism: Accelerating the Development of a Trusted Information Sharing Environment*, we proposed the adoption of a standard of "authorized use" that would enable an individual trying to access information so that they could pursue an area of inquiry to document why they were authorized to use it. In the 2007, 9/11 Commission Recommendations Implementation Act, Congress asked the executive branch to advise whether it thought such a standard was practical. In his March 2008 "Feasibility Report" to Congress, the Program Manager for the Information Sharing Environment (PM-ISE) discussed numerous potential obstacles that he viewed as

[7] Previous Markle testimony is available at http://www.markle.org/national-security/publications-briefs-national-security.

[8] GAO, "High Risk Series: An Update," (Feb. 2011), p. 96, available at http://www.gao.gov/new.items/d11278.pdf (last visited 1 March 2011).

[9] More information on Markle's previous work on authorized use is available at www.markle.org/sites/default/files/20090825_authusestndrd.pdf.

limiting the feasibility of implementing an authorized use standard.[10] None of the objections cited in the report, however, were technical in nature. Commercial, off-the-shelf technology, which continues to become more widely available, enables the use of such a standard even in today's environment of multiple and differing authorities and standards across the government. Again, we believe this standard should be considered.

The authorized use standard, as conceived of by the Markle Task Force, was intended to change information sharing practices in four ways:

1. Information sharing would be based on the specified mission of the receiving office or individual. The threshold question would be whether the requesting agency could articulate a purpose for which the information would be used that was within the specific and authorized mission of that requesting agency. With proper implementation of permissioning systems, that authorized purpose could be specific to a work unit or individual, working a specific problem or threat. The authorized use concept demands clarity of authorized uses; that is, careful consideration of appropriate roles and missions of different agencies, offices and individuals. In our view, it would not be sufficient to claim something as general as "counter-terrorism" or "counter-proliferation" as an authorized purpose. Instead, an authorized purpose would have to be something quite specific, such as "tracing the flow of terrorist financing through the international banking system" or "examining the role of North Korea in the proliferation of nuclear weapons technology."

2. The question of deciding how the information would be used would be based on that objective definition of the mission of the requesting office or individual, rather than the subjective determination by the originator of the requesting entity's "need to know." The originator might still be able to dispute the requesting entity's claim that it had an authorized purpose that it intended to use the information for, but the presumption would be in favor of sharing in response to claims for specific authorized uses, and the adjudication of sharing disputes would be based not on the originator's assessment of need to know but on the adequacy of the asserted authorized use. The concept recognized, of course, that certain information might still not be sharable for security reasons even if an otherwise legitimate authorized use was asserted.

3. Even with clear and consistent guidelines for information sharing, disputes will inevitably arise. Information sharing participants, particularly in the early stages, will confront unforeseen circumstances for which there exists no clear guidance. There also will be differences in interpretation of even the clearest guidelines, particularly when classified or otherwise sensitive information is involved and when agencies have conflicting perceptions of the risks of sharing. The information sharing environment, therefore, must include a systematic, workable, efficient process through which to resolve these disputes. The dispute resolution process can provide practical support to advancing the overarching goal of responsible information sharing.

4. A comprehensive authorized use standard would incorporate a dynamic permissioning process into that standard. That is, if a user seeking classified information cannot make a strong initial case showing that the information is needed for investigation, analysis, or some other important

[10] Program Manager, Information Sharing Environment, "Feasibility Report: Report for the Congress of the United States," March 2008, p. 14.

> purpose, a process for developing more information from less sensitive sources should commence. As more is known about need for information and the risks of failing to share, potential users could return to the dispute resolution process with more information and receive new reviews quickly.

If authorized use procedures such as these had been in place, PFC Manning would have had access to Department of Defense information directly focused on the specific issue he was working on as a military intelligence analyst in Iraq. Manning also would have had access to information relevant to his work produced by other departments in the government. However, Manning would not have had access to the 1.6 gigabytes of data that contained sensitive reporting across the spectrum of US government activities. Authorized use significantly reduces the amount of damage any one individual can do. Thus an authorized use standard should be a critical element of any information sharing system as a tool for mitigating the risks of information sharing.

Moreover, authorized use offers multiple operational benefits. It has the potential to reduce uncoordinated action by different agencies and to substantially decrease the level of noise in the system by targeting those who have and need access to information. It facilitates trust, as users must state their purpose for accessing the information as well as how they plan to use it. And when combined with information discoverability, as discussed below, authorized use is a means to identify others who have an interest in the same person or topic so that an interaction and exchange might begin.

Immutable Audit[11]

Transmitting agencies should be required to keep an immutable, auditable record of each dissemination of information for which an articulation of authorized use was made. Maintaining tamper-resistant logs of user activity in the Information Sharing Environment increases security, builds trust among users, measures compliance with relevant policies and guidelines, and improves both transparency and the ability of stakeholders outside of the system to perform appropriate oversight. Such auditing is helpful for securing information from insider compromise and for protecting civil liberties.

Working under an authorized use standard, if audits were to find that an asserted use is not actually within the assigned mission of the receiving unit or individual, or if periodic assessments determine that information is not being used for an authorized use (or not being used at all), then managers and policymakers have an objective basis for reassessing and perhaps terminating the sharing, thus minimizing the risk of information loss, misuse or abuse.

Real-time audits also would play a role in helping identify unauthorized access and, if the allegations against PFC Manning are true, would have triggered immediate technological and human responses, preventing him from downloading more information and alerting counter-intelligence authorities.

[11] More information about Markle's previous work on immutable audit is available at www.markle.org/sites/default/files/nstf_IAL_020906.pdf.

Auditing these immutable logs would have the added benefit of creating new intelligence and knowledge for analysts, policymakers, and others, as well as facilitating dispute resolution by creating real-time, electronically-accessible records that automated software can use to identify common questions presented by different analysts.

Implementation

Making information sharing more secure should go hand-in-hand with making the information sharing environment more effective and trusted by both those working to protect us and by the American people. Critical additional elements of an effective information sharing system that require further development include deepening government-wide policies for sharing information about US persons, discoverability of information, metrics to assess progress, and sustained leadership to bring change across the entirety of government.

US Persons Policies[12]

Government-wide privacy and civil liberties policies for sharing information about US persons must be deepened to match increased technological capabilities to collect, store, and analyze data. Director of National Intelligence Clapper noted in a recent Threat Assessment delivered to the House Permanent Select Committee on Intelligence that homegrown extremists now "play a disproportionately large role in the threat to US interests because of their understanding of the US Homeland, connections to compatriots back in the United States, and relatively easy access to the Homeland and potentially to US facilities overseas."[13] Furthermore, it is becoming increasingly difficult to distinguish between foreign collection and US Persons collection because of the transnational nature of terror groups.

Progress has been made in understanding how information about US Persons can be collected and used, and the predicates for such use. However, much more work is needed on government-wide policies regarding collecting data on US Persons. Inconsistent interpretation of US Persons law across the government can result in government personnel not taking full advantage of lawful activities because individuals are not certain how the law applies to specific cases. This has led to risk aversion when collecting and sharing critical information about US Persons that might stop terrorist attacks.

Consistent and transparent policies regarding the use of US Persons data are necessary to both empower the participants in the information sharing environment and assure the American people that their civil

[12] More information about Markle's previous work on US Persons policy and other privacy issues is available at http://www.markle.org/sites/default/files/20090717_nstfprivacy.pdf.

[13] Prepared Testimony of James R. Clapper, Director of National Intelligence, before the House Permanent Select Committee on Intelligence, 112th Cong., 1st Sess., 10 February 2011, available at http://www.dni.gov/testimonies/20110210_testimony_clapper.pdf (last visited 1 March 2011).

liberties are being protected by the government. Such policies could help prevent the next intelligence failure based on an agency claiming it was not authorized to use information on US Persons.

Discoverability[14]

Like a library card catalog that offers information on books but not the books themselves, discoverability offers users the ability to discover data without gaining access to the entire record unless or until it is authorized. All data within a distributed information sharing environment should be made "discoverable." Through the use of indexes (the cyber equivalent of library card catalogs), users are able to discover data that exists elsewhere, returning pointers to data holders and documents. Requiring agencies to tag their data is a critical first step toward discoverability.

In addition, systems should be put in place so that data can find data. Data finding data links an arriving piece of information to existing information such that insight will emerge automatically when analyst attention is warranted. This process can be automated using existing technology so that notifications can be sent to users when new data reveals a connection that may warrant attention. Such notifications would help focus the finite investigative resources of the US government (e.g., by highlighting new information for select individuals who have previously expressed interest in a topic, much like when Amazon.com recommends new books based on a user's order history). When data finds data, such a distributed network can empower people at the edges of the system by enabling human collaboration to be directed to the most pressing issues. However, individuals would not have access to the content without further action.

Commercially available technology exists to enable discoverability, and this technology has proven effective on a large scale in numerous private sector applications. In fact, commercial off-the-shelf technology built specifically to enable the government to achieve goals such as discoverability, selective revelation, real-time and immutable auditing, and enforcing an authorized use standard, is in use already at a number of government departments and agencies.

Metrics

Metrics are a critical management tool that can catalyze the further work that is needed to improve government's ability to understand threats and also manage information access. By the 10th anniversary of 9/11, a baseline set of metrics needs to be established so that progress toward discoverability and other key information sharing goals can be quantitatively measured against that baseline. Scores on these metrics should be taken into account in budgetary decisions immediately. Such metrics can help overcome bureaucratic resistance to change by creating significant consequences for inaction.

[14] More information about Markle's previous work on discoverability is available at www.markle.org/sites/default/files/20090825_discoverability.pdf.

Sustained Leadership

As we have emphasized in all the Markle Task Force reports, Presidential leadership continues to be critical for building an effective and reliable information sharing environment. Because information must be shared between and among all levels of government and the private sector, leadership on information sharing must come from the White House, not from a person limited to the intelligence community such as the DNI.

To this end, we have long advocated that the PM-ISE be on the National Security Council staff or be at the Office of Management and Budget. Empowering the PM-ISE at this level increases the potential for the government to stop the next terrorist attack *and* the next unauthorized disclosure.

Conclusion

The 9/11 Commission identified ten lost operational opportunities to derail the 9/11 attacks—and most involved a failure to share information. Progress on information sharing is the single most important step required to improve the national security of the United States. If there is another massive terrorist attack on the United States, the American people will neither understand nor forgive a failure to have connected the dots.

The lesson we should take away from the unauthorized release of classified information to WikiLeaks, then, is not that we should reduce or stop sharing information. Instead, as we develop the capability to better share information, we need at the same time to develop the policies, processes and organizational culture that control access and use. Only by doing this can we build an Information Sharing Environment that those who are working to protect us will trust and use, and that the American people will trust to protect their privacy and civil liberties.