Statement for the Record

before the
Senate Homeland Security and
Governmental Affairs Committee

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

Statement of Corin R. Stone
Intelligence Community Information Sharing Executive
Office of the Director of National Intelligence

10 March 2011

Statement of Corin R. Stone
Intelligence Community Information Sharing Executive
before the
Senate Homeland Security and Governmental Affairs Committee
10 March 2011

Introduction

Chairman Lieberman, Ranking Member Collins, and Members of the Committee, thank you for the invitation to appear before you today to discuss the Intelligence Community's (IC) progress and challenges in sharing information. I want to first recognize the Committee's leadership on these important issues and thank you for your continued commitment to assisting us as we address the many questions associated with the need to both share information and to protect it.

Information Sharing

As the IC Information Sharing Executive (IC ISE), my main focus today concerns classified information – and, in particular, information that is derived from intelligence sources and methods, or information that is reflected in the analytic judgments and assessments that the IC produces. I want to be clear, though, that our concern for the protection of information is not restricted to the fragility of sources and methods, but extends as well to broader aspects of national security. We recognize, and will hear today, that the Departments of State and Defense, as well as other federal agencies, themselves originate classified national security information that is vital to the protection of our nation and conduct of our foreign relations, and this information is, like intelligence information, widely distributed and used throughout the government to achieve these objectives. As we have seen recently, the unauthorized disclosure of any form of classified national security information has serious implications for the policy and operational aspects of national security.

I am acutely aware that our major task is to find what the Director of National Intelligence (DNI) has termed the "sweet spot" between the two critical imperatives of sharing and protecting information. To ensure that we share and protect information effectively, we work to find the "sweet spot," as the compelling need for information sharing remains a top priority for the DNI and the IC.

The need is compelling because information sharing is essential to provide quality intelligence support to such disparate activities as coalition warfare, counternarcotics, counterproliferation, homeland security, and cybersecurity. Intelligence judgments and reports that reflect our commitment to sharing information are also essential to support senior policymakers who must deal with matters of increasing complexity in a world that is interconnected and fast-paced. Every day, the talented collectors and analysts within the IC share vital information with each other, our partners, and customers, to provide critical support to senior policymakers across the Executive Branch and Congress. We have made great strides in the post-9/11 era, especially in the counterterrorism mission. The United States is safer because of the progress we have made –

as a Community and as a Government – in sharing information more effectively and raising "signals" from the "noise."

Our efforts are not a matter of finding a "balance" between the need to share information and the need to protect; that term implies a "zero-sum" relationship that, as we increase sharing, for example, we also decrease protection. We believe it is more accurate to approach this relationship as one that requires coordinated increases in protecting and sharing information. In other words, as we increase information sharing, we must also increase the protections afforded to that information.

With that approach in mind, we are working to ensure that the IC has the policies, practices, and technologies in place to enable the Community to share information, while both protecting the information and safeguarding privacy and civil liberties. It is clear, for example, that a fundamentally important relationship exists between the parallel needs to share and protect information, and the IC's technology systems and networks' ability to securely store and handle that information. But we also recognize that some of the most complex matters that must be addressed as we increase the sharing of intelligence within and beyond the bounds of the IC largely relate to policy, legal, and cultural issues.

IC Information Sharing Executive

To provide additional emphasis in those areas (policy, legal, and cultural), and to move the center of gravity for the IC beyond technologies and systems, the DNI reassigned the IC ISE role from the IC Chief Information Officer to the ODNI's Office of Policy and Strategy in October 2010. As the DNI's appointed IC ISE, I am developing a coordinated and comprehensive plan for responsibly managing information sharing activities within the ODNI, across the IC, and with all of our mission partners.

To that end, I have established an internal governance process for ensuring a coordinated information sharing approach within the ODNI. I have also refashioned and reinvigorated the IC ISE's engagement activities and governance across the IC to do the same, as well as to set IC-wide priorities and oversee their execution. In carrying out these functions and this mission, I am directly accountable to the Principal Deputy Director of National Intelligence. In addition, I have an excellent partnership with the Program Manager for the Information Sharing Environment (PM-ISE), who focuses on sharing information related to counterterrorism and homeland security across the entire U.S. Government. Our close working relationship helps me ensure that the information sharing activities we undertake in the IC related to those areas are consistent and interoperable with the steps being taken across the entire U.S. Government, as well as with our state, local, tribal, and private sector partners. In this partnership, we agree; responsible information sharing remains our top priority.

Finding the "Sweet Spot"

The IC's work on the complicated questions related to access to intelligence, and the ways in which it can be a shared responsibility, pre-dates the recent unauthorized disclosures. The challenges associated with both sharing and protecting intelligence are not new and have been a

factor of major consideration in the Community for years. As this Committee knows all too well, it is one of the foundational principles underlying the Intelligence Reform and Terrorism Prevention Act of 2004, as well as the creation of the Office of the Director of National Intelligence. The latest unauthorized disclosures, however, underscored again the importance of a comprehensive approach to address those challenges.

Working within the broad Government effort that is underway to address the security of classified information in the context of information sharing, the IC's strategy involves three interlocking elements:

- The first is ACCESS: ensuring that the right people can discover and access the networks and information they need to perform their duties, but not to information that they do not need. This is a complex matter that is centered on the principle of determining "Need to Know."

- The second element is TECHNICAL PROTECTION: technically limiting the ability to misappropriate, manipulate, or transfer data, especially in large quantities, such as by disabling or prohibiting the use of removable media on classified networks, including thumb drives and CDs.

- The third area is AUDITING and MONITORING: taking actions to give the IC day-to-day confidence that the information access granted to our personnel is being properly used. This involves monitoring and auditing user activity on classified computer systems to identify anomalous activity, and following up accordingly.

We are also focused on additional measures to protect classified information from "Insider Threats." Consequently, in concert with the three principal elements of our strategy, we must also sustain strong personnel security investigation and reinvestigation programs, ensure that we conduct effective security awareness training, and take or support action against those who disclose classified information without authorization.

Addressing the Insider Threat

The damage caused by the unauthorized disclosures of classified information stems from the actions of individuals and their malicious exploitation of the opportunities available to them in a classified environment. Over the course of our nation's history, there have been spies among us, and the actions of those individuals have demonstrated how a trusted insider "gone wrong" can do grave damage to national security. It is clear that we must be vigilant and proactive in trying to detect, mitigate, and deter this threat.

To meet that challenge, the U.S. Government must have a comprehensive insider threat detection capability. The National Counterintelligence Executive (NCIX) has developed such a program for the IC, and we are working toward implementing its principles. Over the course of the last several months, agencies have worked together to support the development of an insider threat monitoring capability that can be deployed across the entire Government. There are different maturity levels across the Government, and, as a result, improvements will be phased throughout

implementation. Technology refresh is a vital part of this program and is being considered for emerging threats, as well as our technology platform, for sharing and protecting information. A robust insider threat detection program will allow departments and agencies to manage the risk caused by granting broader access to sensitive information in Government.

In structuring and implementing insider threat efforts, however, it is paramount that each department and agency ensures privacy protections are in place, and that access to insider threat detection information and activities are limited to authorized personnel performing counterintelligence, security, and other appropriate oversight missions.

It is also important to note that insider threat capabilities are not intended only to detect or deter potential bad actors. These capabilities are also critical to build and increase confidence that access to intelligence is being properly used and protected. That confidence is essential to building a culture that supports responsible information sharing.

Security

Executive Order 13526 established the Information Security Oversight Office (ISOO) of the National Archives and Records Administration as the oversight organization for safeguarding classified information in the federal government, and gave the DNI responsibility for the oversight of all classified national intelligence information. The ONCIX performs the security oversight function for the IC to ensure that its 17 agencies and elements have effective measures and mechanisms to protect classified national intelligence from unauthorized disclosure, and to ensure that any security barriers to information sharing are necessary.

There has not been a unified process to assess the counterintelligence, security, and information assurance postures within all Executive Branch departments and agencies. Departments and agencies currently assess their own performance and compliance with internal programs and regulations. In coordination with OMB, ISOO and ONCIX will evaluate and assist agencies in their assessments, and plan to use on-site reviews as part of that process.

Technology

A dual-pronged approach is needed to improving technology solutions in the classified information sharing environment: (1) enhancements to logical and physical security controls; and (2) incremental delivery of information sharing capabilities through prioritized mission needs from the intelligence, defense, and civilian agency communities.

Critical capabilities supported by technology – such as identity and access management, data protection and discoverability, and a reliable audit process – play an integral role in the steps we are taking to find the "sweet spot" between the need to share and the need to protect intelligence. In particular, technology can help regulate the availability of information. It can also help to identify and prevent the potential misappropriation, manipulation, or transfer of data; as well as the means by which such actions can be taken. Further, technology can record users' actions and

support the investigation and prosecution of those who intentionally misappropriate classified information. The IC is working to provide end-to-end data management technology to ensure that sensitive intelligence data is appropriately protected throughout its life cycle (creation, use, transit, storage).

To enable strong network authentication and ensure that networks and systems can authoritatively identify who is accessing classified information, the IC CIO is implementing user authentication technologies and is working with the IC elements to achieve certificate issuance to eligible IC personnel in the first quarter of fiscal year 2012. In addition to networks and systems, the IC is working to advance the authentication standards to applications in order to better protect data. Identity management for both networks and applications represent the foundational capability required to enable access management decisions and ultimately the recording or audit of users' actions with attribution.

The IC plans to increase access control to critical IC information resources, based on Data Protection Models in fiscal year 2011-2012. To that end, the IC CIO is standardizing a Data Protection Model based on current and evolving protection requirements and identity attributes. This approach will allow for several levels of protection; from open access through highly restricted availability. The appropriate protection level will vary based on factors such as data sensitivity, environment, mission criticality, and systems capabilities. Important elements in this approach include authentication techniques and the use of attributes (such as clearance level) to determine identities and support mission-based access to intelligence. Access control capabilities ensure that information content is only accessible by those individuals who possess the appropriate need, as validated by their management.

For higher levels of protection, technology can be used to control usage and limit user capabilities to perform activities such as copying, printing, or exporting data to a device. At this level, access requires strong user identification and authentication for system access along with the use of one or more attributes such as clearance level, digital identifier, role, or Community of Interest.

Data discoverability is another vital component to enable sharing while appropriately restricting access to information content. In the event that a user is inadvertently denied access to information needed to perform the mission, yet does not possess the appropriate attributes (for example clearance level, organization, or "Need to Know"), this capability will allow that user to discover the existence of, and request access to, the information

Finally, audit and monitoring technologies are necessary to ensure that employees' access to intelligence information is recorded and anomalies are detectable. Implementation of audit and monitoring technologies, by providing a reliable record of users' actions, will support our ability to identify and react to apparently inconsistent activities, while also affording a means of deterring errant user behavior. During fiscal year 2012, the IC CIO will leverage an Enterprise Audit Framework to enhance the sharing of audit data across the IC elements.

In addition to these critical technologies – identity and access management, data protection and discoverability, and a reliable audit – the IC CIO continues to look at ways to leverage additional

technologies, such as digital management and data loss prevention, to find the "sweet spot" between sharing and protecting intelligence.

Conclusion

The IC is fully committed to giving policymakers, warfighters, law enforcement officers, and our other partners the best intelligence and analytic insight we can provide. This support is essential to enable all those we serve to make the decisions, and take the actions that will protect American lives and American interests, here and around the world.

To carry out that critical mission, it remains vitally important to both share and protect networks, intelligence, and associated information – and the systems and networks that support them. As we continue to increase sharing, we must also increase the protections put in place to heighten confidence that the intelligence and information that is being shared is being properly used and protected. This is a matter of managing risk; and people, policies, processes, and technology all play important and interconnected roles in managing that risk.

Appropriate policies must be aligned across many information sharing constituencies to include, federal, military, state, local, tribal, private sector, and international partners. These policies must also be consistent with the law, and appropriately address civil liberties and privacy concerns. Cultural attitudes and behaviors must reflect these priorities, and be shaped through appropriate training and incentives. Work on the next generation information sharing environment must begin now and be collaboratively developed with the IC and other stakeholder agencies.

Whether classified information is acquired via a computer system, a classified document, or simply heard in a briefing or meeting, we have had "bad apples" who have misused such information before and, unfortunately, we will see them again. That does not mean we should err on the side of not sharing intelligence or information – the risk caused by not sharing the information we have with those who need it is simply too great. Rather, we must put all proper safeguards in place, continue to be forward leaning to find the threat before disclosures occur, be mindful of the risks, and manage those risks in the light of the importance of our mission.