U.S. DEPARTMENT OF THE TREASURY

Press Center

Remarks of Assistant Secretary for Financial Institutions Cyrus Amir-Mokri at the Securities Industry and Financial Markets Association (SIFMA) Conference "Cybersecurity Standards: Exploring the NIST Framework."

3/18/2014

As prepared for delivery

Good morning. Thank you for having me. I commend SIFMA on organizing this seminar dedicated to discussing President Obama's Executive Order 13636 and the cybersecurity framework published by the National Institute of Standards and Technology (NIST). I also commend SIFMA for its more general focus on cybersecurity, and in working with other industry associations and government agencies on these issues.

What I'd like to do today is to outline the basic substantive elements of the NIST Framework and then to offer some thoughts on how our operational activities and policy thinking at Treasury fits with the Framework. I hope that my account will both give you a sense of what we have been doing to help improve the financial sector's cybersecurity resilience and suggest some direction for further policy and operational development.

But I'd like to start with a few fundamental observations about our collective cybersecurity efforts. The first is just that: our cybersecurity efforts are *collective*, and it is important that they remain so. The endeavor is collective along several dimensions. It is, for example, a "whole of government" effort. To illustrate: even though Treasury is the financial sector's "sector specific agency", Treasury can be effective only if it works well with other government agencies, including the financial regulators, law enforcement, homeland security, and the intelligence community. Each agency has particular expertise, responsibilities, and functions, and each agency must communicate and coordinate with the other agencies to make the collective endeavor work.

This collective effort also requires a public/private partnership. As President Obama's Executive Order implies, it is important for the government to share information and provide technical assistance to the private sector. At the same time, as the Executive Order also implies, it is important for the private sector, including firms both small and large, to do its part in maintaining robust cybersecurity resilience and readiness. The private sector should also continue to expand its various collaborations on these issues, whether it is technical collaboration, identifying weak points in the overall system, or sharing threat information.

My second observation is that our vigilance must be persistent and sophisticated because the threats are persistent and increasingly sophisticated. The threat actors can be varied, and their intentions can range from causing inconvenience and embarrassment to doing severe harm to the United States economy. The combination of the threat actors' persistence, sophistication, and motivation means that, probabilistically, we should think and plan not just in terms of resilience and defense, but, as implied by the Framework, also in terms of adjustment, reaction, crisis management, recovery, and business continuity. As applied to the financial system, for example, we should plan with a view toward the interconnectivity of the various participants; if one firm is the victim of a cyber-attack, other firms may also be threatened. We should understand the implications of this interconnectivity -- which could take forms ranging from malware contagion to panic and diminishment of confidence in the financial system -- and prepare accordingly.

Finally, there will be no silver bullets. So long as we rely on information technology in the pervasive way we do today, cybersecurity will remain a priority. We must continuously strive to remain ahead of threat actors. The Framework anticipates this by being flexible. As the authors of the Framework indicate, the Framework is intended to be a "living document" that will evolve based, in part, on feedback from market participants on its implementation.

The NIST Framework

Let me now turn to a few notes on the NIST Framework. President Obama's Executive Order called for public input in developing the Framework. In the days directly after the President issued the Executive Order, Treasury was in communication with the financial sector regarding input into the Framework. Working with the very capable staff at NIST, the financial sector provided important technical and sector-specific knowledge to assist the drafting process. Over the 12-month period from the issuance of the Executive Order to the roll out of the Framework, the financial sector sent representatives to all of the five NIST workshops, convened financial sector specific meetings with NIST and Treasury, and provided comment letters on the draft document. Without this time commitment and sharing of knowledge by

the financial sector and all of the members of the public who devoted time to this subject, the NIST Framework would not have been completed so successfully.

As you all know, the NIST Framework has five basic, or "core", elements: (i) identify; (ii) protect; (iii) detect; (iv) respond; and (v) recover. The Framework itself describes in more detail these core components and the tiers they comprise. What I thought I would do today is explain generally how our efforts map onto these five core elements, and highlight certain areas of these core elements which merit further policy development.

Briefly, as it applies to the financial system, one way to understand the framework is along three broad concepts: (i) front-line resilience; (ii) crisis management; and (iii) recovery and continuity. This is not unlike the framework we typically use in prudential financial regulation, where, for example, we think of capital and liquidity buffers as resiliency tools and the resolution authority as an element of both crisis management and disposition of a firm after insolvency. These three elements map onto the NIST framework as follows. The elements of identify, protect and detect correspond to front-line resilience. The elements of detect and respond are essential to crisis management. Finally, the core element recover corresponds to recovery and continuity.

Front-Line Protection

Front line protection consists of the series of activities that help foil threat actors from either penetrating into a system or from causing damage in the event that they are able to penetrate. This latter point is important: the best thinking on cybersecurity today concedes that some threat actors may be able to penetrate a system. That being acknowledged, it is important for system design to rapidly detect such intrusion, and be designed to prevent lateral movement and ready access to the whole network once a threat actor has penetrated. Most of this effort relies on the expertise of information technology and security professionals. And, given the diversity of systems and systems architecture among financial firms, primary responsibility for identifying key information systems and network functions and for protecting those systems rests with the financial sector itself. But there are some important ways in which government can contribute to front-line resilience, and we have been hard at work on those fronts.

First, as implied by the President's Executive Order, we view sharing threat information with the financial sector as being critically important. Many government agencies collect threat information. To go back to my earlier point about a "whole of government" approach, we have been working on improving both the flow and the quality of information and threat analysis disseminated to the private sector. At Treasury, we have personnel who are dedicated to this task and who communicate continually with their colleagues in other areas of the government -- including law enforcement, intelligence, and homeland security – to better equip the private sector with information that will help them perform the front-line defense function.

Private sector firms also are able to improve resiliency at this stage by increased information sharing with each other. The Financial Services – Information Sharing and Analysis Center has an important role to play as a central hub of information sharing within the sector and between the sector and other private entities and government. We hope to see this already strong institution continue to build capacity through continued support from the sector.

Here, Congress also has its role to play. To improve the level of information sharing that takes place, Congress needs to pass comprehensive legislation that provides liability protections and privacy considerations that encourage the private sector to expand information sharing in an appropriate manner.

Second, and once again as indicated by the Executive Order, since the dissemination of threat information may at times need to be controlled, it is important for appropriate personnel in the private sector to have appropriate clearance. Providing for such clearances has been a priority for us. Consistent with the Framework's evolutionary approach to cybersecurity, we will continually assess the need for clearances and will seek to be sure that, at all times, the financial sector is in a position to receive actionable threat information.

Third, the financial regulatory community can set expectations and perform examinations that help financial firms maintain a baseline for cybersecurity readiness. The Federal Financial Institutions Examination Council (FFIEC), which sets guidelines for its members to conduct supervisory exams with respect to financial firms' information security protocols, has organized a working group to understand how it might better supervise cyber-related concerns. The SEC has also proposed Regulation SCI, which would require SEC registrants to maintain information security policies and procedures, conduct business continuity testing, and provide certain notifications in the event of systems disruptions. We look forward to the SEC finalizing this rule in 2014.

While our principal points of reference so far have been financial firms themselves, we are mindful of the role that third parties play in providing information technology services to financial firms, whether they act as consultants, suppliers, or even participants in the delivery of financial services. Our focus cannot fail to take account of the role of these third parties. In particular, many financial institutions, especially smaller firms, retain technology firms to provide core information security and back-office services. Thus, when we talk about safety and soundness in the context of cybersecurity, we cannot focus solely on financial firms themselves.

Incident Management

As the Framework suggests, each firm ought to have protocols for managing and responding to a significant incident. Given the interconnectivity of the financial system and the structure of markets, however, we in government and in the financial sector must also think about incident management not just in terms of a single firm, but in terms of the financial system as a whole.

We are collectively making important strides in this regard. In government, as indicated in the Executive Order, we are mindful that we should be prepared to provide not just information, but at times also technical assistance. At Treasury, we coordinate the provision of technical assistance for the financial sector with homeland security, law enforcement, the financial regulators, and others.

For cases where there might be effects on the financial system more generally, we must collectively work on communication and coordination protocols. Industry, in collaboration with Treasury, has been working over the past year to improve existing incident management procedures. The FSSCC, for example, is currently working to update its "Cyber Incident Response Plan," which focuses specifically on cyber-attacks. In addition, SIFMA has held tabletop and simulation exercises to test governance, communications, and other incident management protocols. Treasury and the financial regulators have both observed and commented on these exercises.

As we continue to work on and refine our communications protocols, it is important to bear two things in mind. First, within firms, communications between information technology personnel and business decision-makers needs to be seamless. For example, information technology experts need to understand from business decision makers what levels and kinds of impairment in network function may require interruption of services. Similarly, business decision makers need to understand from information security experts what kinds of functions are realistic in the face of a cyber-attack. Second, and for largely similar reasons, in times of crisis, it is critically important for the lines of communication between the private sector and government to be active and clear.

Recovery

The final area I would like to touch upon is planning for recovery, which is the final element of the NIST framework. Recovery consists, first, of restoring systems and services in the event a cyber-attack leads to disruption of services, data corruption or destruction, or entire systems failure. This aspect of recovery is largely driven by information technology expertise. However, there may be scenarios in which information technology cannot restore the data that was corrupted or destroyed. In the context of the financial system, such a situation may require protocols for dispute resolution and other post-crisis management of loss.

As we engage in scenario planning and business continuity design, existing paradigms for physical attacks may not be very relevant. For example, building and maintaining backup systems in different geographies will not necessarily guard against scenarios in which a backup or recovery system itself might be infected by malware. Similarly, because having backup systems in separate geographies largely addresses problems that arise in paradigms of physical loss, they do not allow us fully to plan for interconnectivity effects in the financial system.

These more extreme cyber-attack scenarios accordingly raise the question not only of the technical challenge to recover lost or corrupted information, but also, for example, the question of what principles should govern any dispute resolution that might be attendant to a recovery. While protocols exist and are regularly tested to resolve problems such as broken or canceled trades, we should be sure to test them for instances where we might experience significant data loss or corruption affecting the financial system.

Conclusion

The NIST Framework provides a strong basis for organizing our collective thinking around cybersecurity. While the Framework focuses on describing a protocol for individual firms, it also provides a basis for organizing our thoughts around the collective endeavor of safeguarding the financial system. But as we do so, we must be sure to account for the complexity of safeguarding a system and how it requires the focus and energies of both the public and private sectors. Thank you.