U.S. DEPARTMENT OF THE TREASURY

Press Center

Remarks of Assistant Secretary Cyrus Amir-Mokri on Cybersecurity at a Meeting of the Financial Stability Oversight Council

12/9/2013

WASHINGTON - Thank you, Secretary Lew and members of the Financial Stability Oversight Council, for the opportunity to speak today about cybersecurity, the public sector's role, and our collaboration with the financial services sector.

Our experience over the last couple of years shows that cyber-threats to financial institutions and markets are growing in both frequency and sophistication. The changing-nature of these cyber-threats prompted this Council last year to highlight operational risk, and cybersecurity in particular, as worthy of heightened risk management and supervisory attention.

In response to these threats, the US government and the financial sector have come together to identify financial system vulnerabilities, improve the system's resilience, and refine incident management protocols. I would like to highlight a few features of this collective effort.

First, as is true with other aspects of protecting financial stability, this effort needs to be constant and continuous: there will not be a day where we can sit back and say that our job is done. Some of the reasons why this challenge will be daily are as follows: rapidly changing technology, increasing and expanding reliance by financial companies on technology to perform business and customer interaction functions, the creativity and persistence of would-be cyber-attackers, and the complexity of network architecture. So, while we have made progress in our efforts to protect the financial system, we will always have much work ahead of us.

Second, a public-private partnership in this area is not only desirable, it is necessary. Some of the threats that concern us the most, and that have the potential for creating the greatest harm, are deliberate actions with the intent to cause damage to the financial system. As a result, protection of our financial system can succeed only by combining the resources and capabilities of government with those of the private sector.

Third, this endeavor is about protecting the financial sector as a whole, from the largest financial institutions and exchanges to community banks and credit unions. Accordingly, we work to reach financial institutions of all sizes and business types.

Each stakeholder has an important role to play in this collective endeavor. I'll share with you some key aspects of Treasury's ongoing work on cybersecurity. I will also outline our work to partner with other agencies, regulators, and the private sector to enhance cybersecurity in this area.

Treasury serves as the sector specific agency for the financial sector, which means that it plays a leading role in policy development and a coordinating role in incident response. In this role, Treasury has sought to increase engagement, improve coordination, and facilitate information-sharing on cybersecurity issues with colleagues across the federal government, particularly those involved with national security, homeland security, and law enforcement. We communicate regularly with senior officials in these areas on matters specific to cybersecurity, both in the context of incidents and on more general operational and policy matters.

More specifically, over the past year, Treasury has facilitated detailed cybersecurity briefings, including classified briefings, for both the financial regulatory community and the financial sector. On many occasions, these briefings have been conducted by experts from other agencies. And the audience has been diverse: market utilities such as exchanges and clearinghouses, both large and small banks, insurance companies, credit unions, and asset managers. Briefings have been held across the country through the help of partner agencies, who both have made their regional offices available and have assisted us in conducting the briefings.

We have also collaborated with other agencies, especially law enforcement agencies, on incident response. Treasury's role during an incident often is to facilitate the provision by other government agencies of technical assistance to financial firms.

Treasury is also focused on streamlining the dissemination of information which we receive, notably actionable threat information. To that end, we are continuing to improve our communication with the broader national security community so that we can efficiently receive threat information, analyze and declassify the information as appropriate, and provide it promptly either to affected firms or to the sector as a whole. This function is performed by dedicated personnel whose task is to share information on a regular, timely basis. They are in continual contact with the private sector's FS-ISAC, which is a critical partner in distributing threat information to financial services stakeholders. This partnership with the FS-ISAC is an important building block of the public-private partnership on cybersecurity for the financial sector.

As I've indicated, other agencies in the US government are also active and essential partners in this collective endeavor. The basic concept is at the foundation of the President's Executive Order 13636 on Improving Critical Infrastructure Cybersecurity, issued in February of this year. The Executive Order directs executive branch agencies and departments to work with the private sector to take steps to protect our nation against cyber-threats.

Under the Executive Order, we have been collaborating with other agencies to help the National Institute of Standards and Technology (NIST) develop a framework to protect our critical infrastructure from cyber risks. The Preliminary Framework is currently available for public comment, and the financial regulatory community and the financial sector both have been highly engaged in providing feedback throughout the process.

The work under the Executive Order is vital, but it is not a substitute for cybersecurity legislation. The Administration hopes to work with Congress to ensure our laws keep pace with the evolving threats while protecting privacy and civil liberties. In addition to our work to implement the President's Executive Order, we also work daily with law-enforcement, intelligence, and the Department of Homeland Security on cyber issues.

First, we look to the intelligence community to provide us with threat and vulnerability information. We work with the broader intelligence community to analyze those threats and to share them with the private sector, as appropriate. Second, we work with law enforcement and DHS both to disseminate information to financial firms and to provide technical assistance. Particularly in the case of an incident, we as a government endeavour both to be present at the scene and to offer any assistance we are capable of providing. Third, we look to DHS and other cabinet agencies in cases where events in another sector could affect the financial sector. The experience with superstorm Sandy was instructive for cyber matters. A firm will have difficulty functioning, for example, if there is no electricity or telecommunications, or if its most important resource, its employees, cannot get to work.

Cybersecurity is also a priority for the financial regulators, as this Council has helped to demonstrate. In addition to bilateral Principal briefings, the Council as a whole has been regularly briefed on cybersecurity and other operational risk matters, which were a focus of the Council's 2013 annual report. Broadly speaking, the financial regulators address cybersecurity through regulation and guidance, supervision, and participation in incident response.

Financial regulators are providing guidance to financial firms concerning appropriate governance mechanisms, information security procedures and testing, adequate backup systems, and emergency business continuity and recovery plans. An important goal of these activities is to ensure that each firm under supervision has adequate policies and procedures in place to protect itself from cyber-attacks and potential consequences. For example, the Federal Financial Institutions Examination Council (FFIEC) have over the years established uniform principles and standards for the examinations of financial institutions. The examinations rely on manuals developed by FFIEC for the purpose and on other relevant literature, including publications on information security standards by expert agencies such as the Department of Commerce. Earlier this year, the FFIEC convened a working group to look at updating its approach to supervision and examination specifically with respect to cybersecurity. Another example of activity in this area is the Securities and Exchange Commission's proposed Regulation SCI.

* * *

As the Council appreciates, cybersecurity is a complex subject. Given the nature of the threat and its potential sources, it can be addressed only through a whole-of-government approach combined with a strong public-private partnership. That is both the essence of the President's Executive Order and the summation of our collective efforts. We have made substantial progress with our government and private sector partners to organize our protection of the financial system. However, cyber-threats are here to stay, and we must continually remain vigilant to their ever-evolving character. Thank you for the opportunity to address this important issue before the Council.

###