U.S. DEPARTMENT OF THE TREASURY

Press Center

In Call To Action, Treasury Secretary Lew Urges U.S. Financial Sector To Redouble Efforts Against Cyber Threats

7/16/2014

New York – U.S. Treasury Secretary Jacob J. Lew today urged financial institutions and firms to take critical steps to better protect consumers and strengthen the nation's defenses against cybersecurity thefts, disruptions, and attacks. In remarks at CNBC and the Institutional Investor's 4th Annual Delivering Alpha Conference, Secretary Lew specifically called on the U.S. financial sector to improve cybersecurity by using the Administration's new cybersecurity framework for their own systems and as a way to evaluate outside vendors.

"The consequences of cyber incidents are serious," Secretary Lew said in his remarks. "When credit card data is stolen, it disturbs lives and damages consumer confidence. When trade secrets are robbed, it undercuts America's businesses and undermines U.S. competitiveness. And successful attacks on our financial system would compromise market confidence, jeopardize the integrity of data, and pose a threat to financial stability."

The Treasury Department has been closely involved with the implementation of the 2013 Executive Order 13636, titled "Improving Critical Infrastructure Cybersecurity," and Presidential Policy Directive-21 (PPD-21). Treasury has worked closely with the Commerce Department, other agencies and the private sector to develop a cybersecurity framework that provides a voluntary blueprint that private sector firms of all sizes can use to collaborate with the government, improve the resiliency of their computer systems, and implement global standards in cybersecurity best practices.

While the framework is an important milestone, much more work needs to be done to increase our vigilance against cyber threats. Today, the Secretary also repeated his call for Congress to pass comprehensive legislation to improve information sharing by providing targeted liability protections while protecting privacy considerations.

"As it stands, our laws do not do enough to foster information sharing and defend the public from digital threats. We need legislation with clear rules to encourage collaboration and provide important liability protection. It must be safe for companies to collaborate responsibly, without providing immunity for reckless, negligent or harmful behavior. And we need legislation that protects individual privacy and civil liberties, which are so essential to making the United States a free and open society. We appreciate the bipartisan interest in addressing this important issue, and the Administration will continue to work with key stakeholders on the various bills that are developing in Congress," added Secretary Lew.

As the federal agency responsible for the financial services sector, the Treasury Department continues to work with stakeholders in the private sector as well as the government to enhance the security of the financial sector against cyber incidents and threats. Secretary Lew visited Verizon's cyber threats command center in Virginia yesterday, and today he will meet with members of the Securities Industry and Financial Markets Association and leaders from the financial services industry in New York City to discuss the cybersecurity issues facing critical financial services infrastructure. Additionally, Treasury's Deputy Secretary, Sarah Bloom Raskin, will begin a series of meetings with federal financial regulatory agencies and trade associations comprised of state financial regulatory agencies to reduce cybersecurity risks to the financial system. She will be looking beyond traditional financial services to explore the regulatory, security, and inclusion aspects of financial technology.

Read Secretary Lew's full remarks from the Delivering Alpha Conference here.

The Treasury Department's Role in Financial Sector Cybersecurity

Through the Office of Critical Infrastructure Protection and Compliance Policy (OCIP), the Treasury Department is responsible for facilitating collaborative efforts with the private sector and government agencies to enhance the financial sector's security and resilience.

- **Executive Order 13636 and Presidential Policy Directive-21 (PPD-21):** In February 2013, President Obama released Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity and PPD 21, which directed the Executive Branch to take key actions to enhance the cybersecurity of critical infrastructure companies and advanced a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

- **NIST Cybersecurity Framework:** These actions include developing the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*, which was released in February 2014. This framework provides a blueprint that firms of all sizes can use to evaluate, maintain, and improve the resiliency of their

computer systems. Secretary Lew is calling on all financial firms to use this framework.

Ongoing Efforts:

- **Cyber Intelligence Group:** Treasury has also established the Cyber Intelligence Group (CIG), which shares timely and actionable cybersecurity information that financial institutions can use to protect themselves. The CIG coordinates closely with the Financial Services Information Sharing and Analysis Center (FS-ISAC), established by and for the financial services sector, in this capacity. To date, the CIG has produced 23 circulars containing cyber threat indicators and responded to dozens of requests for information to help the sector prepare for potential threats.

- **Financial and Banking Information Infrastructure Committee (FBIIC):** Treasury chairs this committee of federal financial regulators and membership organizations of state financial regulators to facilitate coordination on critical infrastructure matters. Deputy Secretary Raskin will call on her counterparts to participate regularly in FBIIC meetings.

Going Forward:

- **Improved Information Sharing:** The Treasury Department is working with the Department of Homeland Security, law enforcement agencies, and the Intelligence Community to ensure that relevant and timely threat information, reaches the broadest audience, including smaller firms.

The Treasury Department will:

  - foster additional information sharing between industry and government partners, including by encouraging the private sector to share more information about incidents impacting their systems directly with government and through the Financial Services Information Sharing and Analysis Center (FS-ISAC);
  - work closely with government partners to continue to enhance processes for sharing sensitive government information as broadly as possible; and
  - promote efforts to automate information sharing processes.

- **Industry Adoption of the NIST Framework for Both Firms and Vendors:** The Treasury Department believes the NIST framework is an important and useful blueprint that firms of all sizes can use to evaluate, maintain, and improve the resiliency of their computer systems. This framework, which was released in February, will help create a common language and a set of common practices across different companies and sectors.

The Treasury Department will:

  - encourage every financial services firm to use this framework to reduce cybersecurity threats;
  - promote similar use of the framework by outside vendors and counterparties; and
  - contribute to ongoing efforts to continuously grow and enhance the framework.

- **Regulatory Focus on Cybersecurity:** Treasury applauds the efforts of bank and securities regulators that are taking steps to enhance their oversight to meet the challenges presented by cybersecurity. Notably, the Federal Financial Institutions Examination Council (FFIEC) has established a working group to further promote coordination across the federal and state banking regulatory agencies on critical infrastructure and cybersecurity issues. This summer FFIEC member agencies are conducting a cybersecurity assessment during regularly scheduled exams aimed at improving cybersecurity risk management at community institutions.
- **Interdependence across Sectors:** Given the complexity of our financial system, catastrophic vulnerabilities are not limited to banks. Risks to the system can be found at the vendors, suppliers, and contractors that keep our financial system running. They can be found within industries that underpin the markets—like telecommunications and energy. And they can be found across the physical infrastructure that supports the U.S. economy, like our transportation system and water supply.

The Treasury Department will:

  - work with leaders in the cybersecurity community to identify and mitigate the risks associated with cascading impacts of a cyber-incident;
  - continue to collaborate closely with agencies like the Department of Homeland Security and the Department of Energy so we can coordinate our efforts and make our economy more resilient to cyber-attacks; and
  - enhance and expand information sharing about incidents of mutual interest.

- **Cybersecurity Legislation:** Congress must pass legislation to improve information sharing by providing targeted liability protections while protecting privacy considerations. We continue working with Congress and outside stakeholders, such as privacy advocates and industry, to ensure that evolving information sharing legislation aligns with the Administration's principles.

Legislation should adhere to three key priorities:

  - carefully safeguard privacy and civil liberties;
  - preserve the long-standing, respective roles and missions of civilian and intelligence agencies; and

- provide for appropriate sharing with targeted liability protections.

###