Testimony of Assistant Secretary Daniel L. Glaser
House Foreign Affairs Committee
Confronting North Korea's Cyber Threat
Tuesday, January 13, 2014

Chairman Royce, Ranking Member Engel, and distinguished members of this Committee, thank you for inviting me to speak today about the U.S. Government's efforts to counter the threat posed by the malicious cyber activities of the Democratic People's Republic of Korea (DPRK).

In my remarks today, I will describe the Department of the Treasury's financial tools related to the DPRK and how we are deploying them. I will also discuss Treasury's ongoing efforts to help support the security, resilience and stability of the U.S. financial sector.

DPRK Sanctions

The DPRK is a brazen and isolated regime that has repeatedly shown flagrant disregard for international law and standards. This is evident in the DPRK's development and proliferation of its illicit nuclear and ballistic missile programs, its repeated violations of United Nation Security Council resolutions, its repression of the North Korean people through serious human rights abuses, and, most recently, its cyber-attack on a U.S. company and attempts to stifle freedom of expression in our country.

In response to the DPRK's cyber-attack on Sony Pictures Entertainment (SPE) as well as numerous other egregious acts, the President signed an Executive Order (E.O. 13687) on January 2, 2015 granting Treasury the authority to impose sanctions against officials of the Government of the DPRK or the Workers' Party of Korea (WPK), as well as agencies, instrumentalities, and entities controlled by them and those acting at their direction or on their behalf. The President took this step in furtherance of the United States' commitment to hold the DPRK accountable for its destabilizing, destructive and repressive actions, particularly its efforts to undermine U.S. cyber-security and intimidate U.S. businesses and artists exercising their right of freedom of expression.

E.O. 13687 represents a significant broadening of Treasury's authority to increase financial pressure on the Government of the DPRK and to further isolate the DPRK from the international financial system. With the issuance of E.O. 13687, Treasury, for the first time, has the authority to designate individuals and entities based solely on their status as officials, agencies, instrumentalities, or controlled entities of the Government of the DPRK or the WPK. Treasury also now has the authority to designate those acting on their behalf or providing them with material support. Simultaneous to the issuance of E.O. 13687, Treasury designated three entities and ten individuals whom Treasury Secretary Jacob Lew described as "critical North Korean operatives." These included:

- The Reconnaissance General Bureau (RGB) – the DPRK's primary intelligence organization and responsible for many of its major cyber operations;

- The Korea Mining Development Trading Corporation (KOMID) – the DPRK's primary arms dealer;

- Korea Tangun Trading Corporation – the agency responsible for the procurement of technologies that support the DPRK's defense research and development programs; and

- Ten officials of the DPRK government, including eight KOMID officials based throughout the world and one Tangun official.

Secretary Lew also made it clear that "we will continue to use this broad and powerful tool to expose the activities of North Korean government officials and entities."

While Treasury's authority to target the DPRK Government was expanded significantly under E.O. 13687, Treasury has used existing tools under two other E.O.s to raise the cost to the DPRK of its provocative and illegal actions. Since 2005, Treasury has used its global WMD proliferation E.O. to designate fifty-four DPRK-related entities and individuals under E.O. 13382, which targets individuals and entities engaged in WMD proliferation-related activities. Since August 2010, Treasury has issued nine designations under E.O. 13551, which targets individuals and entities facilitating North Korean arms sales, the procurement of luxury goods, and illicit economic activities. Under these authorities, Treasury has exposed and cut off direct access to the U.S. financial system to entities and individuals such as:

- The Foreign Trade Bank (FTB) and Daedong Credit Bank: two key North Korean banks, both of which provided crucial financial support to DPRK entities responsible for a number of the DPRK's illicit activities, including KOMID;

- General Kim Yong Chol: the head of RGB whom Director of National Intelligence James Clapper recently named as the North Korean official who likely ordered the cyber-attack on SPE; and

- O Kuk Ryol: a Vice Chairman of the North Korean National Defense Commission who previously headed the WPK Operations Department, where he ordered the establishment of a nuclear research and development organization directly under his control.

I should note the importance of coordination with our international partners, particularly those in the region who share our concerns over the DPRK's destabilizing actions. Of course, we will always take the actions we deem necessary to safeguard the United States, our companies, and our financial system. We do, however, recognize that our financial measures are more powerful and effective when undertaken in a multilateral framework. This is certainly the case in the context of the DPRK, which is much more dependent on regional actors than on the United States for its economic survival. Treasury has worked hard with our partners in the region to bring greater pressure to bear on the DPRK. We have seen the fruit of this work in a number of instances of sanctions harmonization, most notably in the case of FTB, where Japan and Australia followed suit in designating FTB. Moreover, some key regional banks, including Chinese banks, severed their ties with FTB after its designation by Treasury.

Today, the DPRK government is financially isolated, thanks, in no small part, to the actions I have described above. Over the years, Treasury has ensured that the DPRK has limited access to the U.S. financial system and worked with our allies to restrict Pyongyang's access to the international financial system. As a result of sanctions and other measures targeting the DPRK's illicit conduct, financial institutions around the world began severing their ties with the DPRK in order to avoid entanglement in illicit activities. These actions contributed to the DPRK's economic isolation and spurred positive change in the behavior of banks across the international financial system. While this increased isolation has made targeting the DPRK more complex, Treasury has continued to use its sanctions authorities to ratchet up the pressure on the DRPK. For now, the DPRK remains defiant, continuing its well-documented illicit activities. As long as this is the case, Treasury will continue to deploy the tools at its disposal to raise the financial cost of such behavior and induce the government of the DPRK to abide by its international obligations. The U.S. government's response to the malicious SPE cyber-attack through E.O. 13687 is a demonstration of our determination to hold the DPRK responsible for its actions. The Treasury Department will continue to use E.O. 13687 and its other sanctions authorities to target the illicit activities of the DPRK.[1]

Promoting the Security and Resilience of the U.S. Financial Sector

Beyond our specific response to the SPE cyber-attack, combatting the threat posed by state-sponsored malicious cyber activity emanating from the DPRK and more broadly is one part of Treasury's broader mission to protect the U.S. financial system, including its critical infrastructure, against illicit misuse and national security threats. To safeguard the U.S. financial system from cyber threats, Treasury pursues a strategy of partnering with the financial sector to share specific threat information, improve baseline security, and enhance industry response and recovery.

In 2013, the President issued Presidential Policy Directive-21 (PPD-21) to strengthen and maintain secure, functioning, and resilient critical infrastructure across industries, and affirmed Treasury's role as the "Sector Specific Agency for Financial Services." In other words, Treasury is charged with helping ensure the security and resiliency of the financial system's infrastructure. This is a tremendous task, given that the United States has thousands of financial institutions and that finance and insurance sectors represent nearly eight percent of our annual GDP.

To most effectively achieve our objectives, robust engagement with interagency partners and the private sector is essential. Treasury chairs the Financial and Banking Information Infrastructure Committee, a standing committee of federal and state financial regulators that coordinates efforts to improve the reliability and security of the U.S. financial system. Treasury also works closely with individual firms, trade associations, and the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security to discuss physical and cyber

[1] In addition to taking action to counter the threats from the DPRK directly, Treasury has also used its tools to defend the U.S. financial sector from cyber threats more broadly under both the Bank Secrecy Act and our sanctions authorities. Prominent examples include our 2013 identification of Liberty Reserve, a virtual currency system that facilitated an estimated $6 billion worth of illicit web-based activity, as a primary money laundering concern under Section 311 and our designation of two malicious Iranian cyber actors under two separate sanctions authorities just last month.

security policy. Treasury further leads the Bank Secrecy Act Advisory Group , comprised of high-level representatives from financial institutions, law enforcement agencies and regulatory authorities to ensure that the Bank Secrecy Act is being administered in the most effective and efficient way. Key topics discussed have included network security, regulatory oversight and cyber threats to the sector.

On a daily basis, Treasury promotes cybersecurity information-sharing with the financial sector and other government entities including the Department of Homeland Security. Sharing such information is critical to enhance firms' abilities to protect their networks and systems from malicious cyber activity, effectively detect and limit the impact of cyber incidents that have already occurred, and establish shared awareness of cyber threats. Treasury's Office of Critical Infrastructure Protection and Compliance Policy (OCIP), in coordination with Treasury's Office of Intelligence and Analysis and interagency partners, identifies, declassifies, and shares timely and actionable information, including threat indicators, to the financial services sector through OCIP's Financial Sector Cyber Intelligence Group.

Treasury's Financial Crimes Enforcement Network (FinCEN), as the administrator of the Bank Secrecy Act, also plays an important role in receiving, analyzing, and sharing information with the private sector related to cyber activity. Based on the financial intelligence that it receives from financial institutions, FinCEN issues advisories to financial institutions, which can help to deter illicit cyber activity and provide information useful to law enforcement. Just last month, based on financial intelligence gathered, FinCEN issued a non-public report to inform financial institutions of the risks associated with Tor networks and to assist them in their efforts to combat cybercrime affecting the sector, such as the malicious use of darknets.

Conclusion

As the United States confronts the destabilizing and destructive actions of the DPRK, Treasury is employing its authorities to isolate North Korea from the international financial system. Treasury will continue to use its arsenal of financial measures to combat the cyber threat posed by the DPRK.