Written Testimony of
Sanjeev "Sonny" Bhagowalia
Deputy Assistant Secretary for Information Systems and Chief Information Officer
United States Department of the Treasury
Before the Subcommittee on
Information Technology of the
Committee on Oversight and Government Reform
United States House of Representatives

## Introduction

Chairman Hurd, Ranking Member Kelly, and members of the subcommittee, thank you for the opportunity to testify today on the Department of the Treasury's procedures and approach to the detection, response, and mitigation of cybersecurity vulnerabilities.

Cybersecurity is one of the top priorities at the Treasury, not only for the Office of the Chief Information Officer (OCIO), but also for our senior leadership at both the department and bureau levels. Like others in the public and private sectors, Treasury relies on technology to meet our mission of serving the American taxpayers and acting as a steward of the national economy. Trillions of dollars and millions of records are stored and processed using Treasury IT systems. We devote a great deal of time, effort, and resources towards securing those systems in order to successfully execute our mission and maintain the trust of the American public.

Our adversaries in the cyber realm make this an increasingly difficult task, but one at which we must continue to succeed. Those targeting our people and our systems continue to grow in their sophistication, resources, and determination. According to a GAO official, cybersecurity incidents reported to the U.S. Computer Emergency Readiness Team (US-CERT) by all federal agencies increased more than 1,000 percent between 2006 and 2014.[1] Treasury's incidents have grown by a far smaller percentage over that same time period. However, Treasury is observing what the rest of U.S. industry and U.S. government has observed: cyber activity by our adversaries is growing in sophistication, volume, brazenness, frequency and potential impact. For example, each year we monitor hundreds of millions access attempts and millions of potentially malicious cyber events. In response to this ever-changing threat, we must continue to be vigilant against the *next* incident, not just the last one. We have improved our cybersecurity posture through a holistic approach of people, process (including policy and governance) and technology. We have also increased our spending on cybersecurity in the past few years to reflect the seriousness of the threat. Our Cyber Enhancement Account in the FY 2017 President's Budget reflects our ongoing commitment to transparency and judicious use of resources as we augment Treasury's cyber defenses. We are continuously and incrementally improving in management and oversight of our IT environment including cybersecurity. We are leveraging synergy opportunities across the enterprise through legal authorities (e.g., FITARA, FISMA, and the Clinger-Cohen Act) to more effectively use our people, processes, technology in the cyberspace.

[1] *Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies*, 7 (2015) (testimony of Gregory C. Wilshusen, Director, Information Security Issues).

Detecting and mitigating vulnerabilities in our environment before they are exploited by our adversaries is an essential component of Treasury's "defense-in-depth" strategy. Having the tools and processes to identify and close these potential holes, and the communication lines to spread the message across government and to our private sector partners, are the keys to effective threat mitigation.

I have divided my testimony into two parts, to answer the two questions posed by the subcommittee. The first part of my testimony will explain how we tackle this challenge at the Department of the Treasury. The second part of my testimony will outline how we participate in the government-wide federal cybersecurity community and support the lead agency for cybersecurity, the Department of Homeland Security (DHS).

## I. Vulnerability Detection, Reporting, Response and Mitigation within Treasury

### The Treasury Environment

As you know, the Department of the Treasury and its bureaus have widely varying missions requiring widely varying IT environments. Our department is a large, geographically and technically diverse enterprise. From the industrial focus of the U.S. Mint and Bureau of Engraving and Printing, to the massive data storage and analytics focus of the Internal Revenue Service, to the advanced economic modeling performed in the Departmental Offices, each Treasury bureau requires a different mix of technologies to accomplish the overall Treasury mission.

While Treasury bureaus are empowered to make the IT decisions necessary to execute their individual missions and carry out many of the operational security functions within their environments, the Treasury CIO is accountable to ensure that those decisions properly consider security implications and evaluate risk and vulnerabilities on an ongoing basis. To this end, Treasury has aligned our departmental cybersecurity strategy with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the OMB Cybersecurity National Action Plan (CNAP) to ensure a common understanding of our objectives across the enterprise. Treasury is fully supportive of the five-part NIST framework (identify, detect, protect, respond and recover) and is proceeding with a department-wide effort to implement all applicable portions of the CNAP. Vulnerability management is part of the NIST framework.

We follow the maxims that "cybersecurity is about risk management" and "if everything is a priority, nothing is a priority." Therefore, we must often make strategic decisions regarding where we should focus our efforts. To the extent possible, and especially in instances where time is of the essence, Treasury employs a risk-based approach to vulnerability remediation. Given the realities of a limited resource environment, Treasury and its bureaus start by remediating vulnerabilities on assets with the greatest risk exposure first, and move systematically to remediate the remaining assets. In addition to security risk, factors such as the operational risk posed to the business are evaluated during the remediation process. This prioritization enables bureaus to focus on fixing the most important vulnerabilities first while facilitating our ability to perform the mission of Treasury.

**Vulnerability Detection**

IT companies, government agencies, security researchers, and others identify thousands of security weaknesses each year in the devices and software that we all use on a daily basis. There are over 76,000 identified vulnerabilities in the National Vulnerability Database. In 2015 alone, over 6,000 new vulnerabilities were added to the database.[2] Critical vulnerabilities are a far smaller number and may represent weaknesses with respect to external or internal threats.

Vulnerability detection requires a multidimensional approach involving asset management, automated tools, monitoring of communication channels, and human analysis. Using each of the multidimensional approaches, Treasury identifies vulnerabilities in our environment that adversaries might exploit.

The foundation of good comprehensive vulnerability detection begins with understanding how the hardware and software is used throughout an organization through strong asset management. Employing this approach allows us to evaluate the impact of each new vulnerability announcement against the equipment in our environment. To this end, Treasury has policies in place requiring our bureaus to perform regular asset and vulnerability inventory scans using automated tools.

In addition to understanding the makeup of our IT environment and performing automated scans against known vulnerabilities, it is critical that we become aware of new vulnerabilities as quickly as possible after they are discovered. Treasury maintains a central security operations center (Treasury SOC) responsible for coordinated department-wide activity that operates around the clock working closely with bureau SOCs and security operations personnel to ensure protection of the department's IT assets. As one of its key functions, the Treasury SOC monitors classified and unclassified government channels, as well as open source and industry channels, for news of critical vulnerabilities and actively participates with other U.S. Government SOCs. Once critical vulnerabilities are identified, the Treasury SOC rapidly transmits the information to Treasury bureaus through alerting and notification channels. Bureau IT operations personnel assess the risk posed by the identified vulnerability to their respective networks and plan mitigation as appropriate, coordinating with the Department OCIO, who maintains overall oversight responsibility under FISMA and FITARA.

Additionally, the Treasury SOC and bureau security teams assess our collective ability to detect and block malicious activity targeting a given vulnerability. Whenever possible, new signatures or indicators are added to Treasury's defensive measures to mitigate risk or respond to any negative impact that may have occurred while the vulnerability was exposed.

Treasury also takes steps at both the enterprise and bureau levels to identify vulnerabilities that our automated scanning may not discover. Some of these countermeasures include penetration testing to uncover configuration or software and hardware vulnerabilities that hackers could exploit, as well as analyzing the attempts against us to identify patterns that may indicate a "zero-day," or undiscovered, vulnerability.

[2] https://nvd.nist.gov/

**Response, Reporting, and Mitigation of Known Vulnerabilities**

To keep up with the thousands of vulnerabilities and associated patches that are released and may apply to their respective environments, the initial response by bureau IT organizations is to undertake a risk analysis for each new vulnerability. Informed by the risk analysis, bureau IT organizations schedule testing and patch deployment as appropriate. This risk analysis aligns with best practices and typically is highly technical and detailed. Factors that bureau IT organizations may consider include the version and current patch levels of vulnerable software running on our hardware, as well as whether the software is configured to block the use of exploitable services and whether other defenses are in place or can be instituted to reduce the likelihood of an exploitable vulnerability. These security concerns are then balanced with operational assessments and testing to mitigate potential business impact that could result from deploying any patches.

A risk analysis may result in several mitigation approaches, such as patching, instituting compensating security controls, or migrating to a new software or hardware solution. These mitigation techniques are then evaluated through follow-on efforts. Compensating security controls may be assessed by a security professional, or automated tools used to scan and assess whether or not patches have been successfully applied throughout the department. This risk analysis and mitigation process covers the vast majority of patching and remediation efforts, and each Treasury bureau manages the timing and nature of the mitigation based on their established risk thresholds.

Bureaus are required to report a set of metrics on vulnerability assessment and remediation to OCIO on a monthly basis, including statistics on percent of assets scanned for known vulnerabilities, and statistics on patch implementation. Additionally, for certain highly important or highly critical vulnerabilities as determined by a risk analysis at the Treasury OCIO, remediation progress is tracked closely by OCIO.

The recent Juniper vulnerability offers an example of this process in action. Within a couple of hours after the vulnerability was announced by the equipment manufacturer, the Treasury SOC alerted bureau-level SOC counterparts to the vulnerability and to the mitigation instructions provided by the vendor. Additional updates and details from DHS were also transmitted to bureaus as they were received. Thanks to the quick action of the Treasury SOC and the bureaus' SOCs, remediation was already under way by the time government-wide alerts to patch vulnerable appliances were issued. Throughout the process, the Treasury SOC and OCIO gathered regular updates on remediation efforts via data call, which were communicated to DHS and Treasury leadership until the vulnerability was fully patched. For any highly critical vulnerabilities, the Treasury SOC and OCIO continue to monitor the remediation status until all the vulnerable assets are patched.

Some notable milestones in this mitigation effort across Treasury include:

- Treasury coordinated an enterprise-wide response to the Juniper vulnerability and patch within a couple of hours of receiving the information from open source vendor channels and DHS;

- Treasury fixed 25% of the patches in a day; 84% within a week; 86% within two weeks; and 93% in seven weeks;
- After a detailed analysis determined that two bureaus configurations posed low risk for exploitation of the vulnerability (because infected devices were not connected to the Internet and thus were not directly affected by the vulnerability and each had multiple compensating controls in-place) Treasury completed the remaining 7% of patching in just over eight weeks;
- DHS NCCIC submitted a notice to all agencies in the U.S. Government indicating close-out of the action on February 17, 2016;
- Treasury submitted the official status of the program to Congress on March 4, 2016.

Table 1 accompanying this testimony illustrates the timeline followed by Treasury in mitigating the vulnerability.

All organizations, both in the public and private sectors, face the same challenge in defending against the asymmetric nature of cyber incidents. To guarantee successful defense of our systems, we must be perfect 100 percent of the time; to penetrate our defenses, while our adversaries only need to succeed once. Federal government organizations face additional challenges working within the restrictions of a two-year budget cycle, compliance with a long list of regulations to defend against adversaries who may change tactics at Internet speed with a singular focus. It is noteworthy that many breaches outside Treasury have exacerbated our cyber efforts, as they have for many agencies across Government.

## II. Treasury's Role in Government-Wide Vulnerability Detection, Response and Mitigation

### Participation in Government-wide Vulnerability Mitigation

First, I would like to start by thanking DHS for their leadership role in federal government cybersecurity. As a member of the federal cybersecurity community, Treasury does its part to support the efforts of DHS and others to identify and remediate critical vulnerabilities. Treasury is an active participant in information sharing efforts, including the Automated Indicator Sharing program, the Cyber Response Group (CRG), and the Cybersecurity Coordination, Assessment, and Response (C-CAR) program. While programs such as C-CAR are instrumental in providing notifications regarding critical vulnerabilities across government, the speed at which our adversaries can identify and exploit vulnerabilities in our infrastructure makes rapid alerts all the more essential. Treasury also has a vast network across government and industry to share cybersecurity practices and lessons learned. Treasury has also engaged with DHS for penetration testing, Remote Vulnerability Assessments (RVA) for high value assets; exchanges information with the law enforcement and intelligence communities for threat awareness; fully participates in the DHS EINSTEIN program and looks forward to participating in the EINSTEIN 3A program; and uses world-class cyber organizations to independently assess our cyber posture.

Another challenge faced by large agencies in complying with government-wide mandates to address particular vulnerabilities is the need to balance operational and security risk. In many cases the devices that must be patched are part of complex systems with several legacy components that may not be compatible with a given security fix. If other security measures can

mitigate risk while a patch is tested for interoperability with a particular system, that factor should be considered in reporting. As much as feasible, government-wide reporting on remediation compliance should factor in risk mitigation as well as raw patching numbers.

I would also like to share a success story of government working together to collectively improve our cybersecurity. In May 2015, DHS issued Binding Operational Directive 15-01, to mitigate the most critical vulnerabilities currently identified on Internet-accessible systems for all Federal Civilian Executive Branch Departments and Agencies. They detected 363 initial active critical vulnerabilities (external) across the Federal Civilian Executive Branch and Departments and Agencies reduced this initial set to two; a 99% reduction. Treasury fully participated in that initiative, reducing to and maintaining our number at zero.

**Continuous Diagnostics and Mitigation (CDM) at Treasury**

The Continuous Diagnostics and Mitigation (CDM) program led by DHS will help move Treasury and other departments and agencies from federated compliance to integrated continuous monitoring by implementing new technologies in three phases. Phase 1, which is currently being implemented at Treasury, will focus on managing our assets and identifying and prioritizing their vulnerabilities. Treasury is an enthusiastic participant in the CDM Program. Later phases will focus on managing our users and managing security events.

Treasury expects that CDM will lead to improved situational awareness regarding vulnerabilities in our environment. When a new vulnerability is discovered, Treasury will have a single data repository containing near real-time information about our entire asset inventory to analyze in order to more quickly assess our risk exposure. CDM will also enable better automation of vulnerability mitigation tracking in near real-time, reducing or eliminating in some cases the need for manual reporting of patch deployment through data calls. This will allow our staff to focus on assessing risk and remediating vulnerabilities rather than just reporting on them.

**Conclusion**

While Treasury has established a solid procedural and operational foundation to identify and mitigate vulnerabilities, our adversaries are constantly changing their methods, and we must remain vigilant to stop them. Continued collaboration with DHS, OMB, and the Congress on improved and streamlined notification as well as standardized toolsets through CDM will enable Treasury to more quickly learn of new vulnerabilities, as well as identify and remediate the affected aspects of our infrastructure.

Treasury understands that better use of our existing resources and strategic deployment of resources are just as important as new funding. Successful implementation of the Federal Information Technology Acquisition Reform Act (FITARA) provides opportunities for improvement in cybersecurity. FITARA can help to reduce the variance in IT asset profiles deployed across the agency, leading to faster mitigation of known vulnerabilities on common platforms. FITARA also enables us to better understand cybersecurity spending across the organization and identify opportunities for efficiency, allowing us to be better stewards of the public funds we already have rather than requesting additional support. Treasury secured full

approval of our FITARA plan in December 2015 and will be reporting significant strides in our April report, thanks to on-going comprehensive reviews of major programs (including cyber).

Protecting against cyber intrusions remains a rapidly evolving challenge. In addition to the challenges and plans I already discussed, I see opportunities where Congressional support could aid our efforts:

1. First, hiring and retaining cyber security staff remains a challenge. We ask for continued support to streamline hiring and offer appropriate incentives to attract and retain that talent.
2. Finally, we ask for your consideration of our FY 2017 budget request for a Cybersecurity Enhancement Account, which will enable us to keep pace with the rapidly evolving adversaries through targeted and accountable spending.

Thank you for your attention to the important subject of vulnerability identification and remediation. I appreciate this opportunity to testify today and I will be glad to answer any questions you may have.

**Table 1: Juniper Vulnerability Remediation Timeline**

| | Date | | | | | | |
|---|---|---|---|---|---|---|---|
| | 17-Dec | 18-Dec | 23-Dec | 15-Jan | 4-Feb | 14-Feb | 17-Feb |
| Days Elapsed From Announcement | Juniper and DHS Announces Vulnerability | 1 | 6 | 29 | 47 | 59 | DHS/NCCIC Issues Event Close-Out |
| High-Risk Devices Patched | | 14 | 40 | 40 | 40 | 40 | |
| Low-Risk Devices Patched | | 0 | 8 | 11 | 13 | 17 | |
| **Total Patched** | | 14 | 48 | 51 | 53 | **57** | |
| **% Complete** | | 24.56% | 84.21% | 89.47% | 92.98% | **100.00%** | |