ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051

http://oversight.house.gov

November 10, 2014

The Honorable Patrick R. Donahoe
Postmaster General and Chief Executive Officer
United States Postal Service
475 L'Enfant Plaza SW
Washington, D.C. 20260

Dear Postmaster General Donahoe:

I am writing to request additional information about the cyber-attack announced publicly today by the Postal Service.

First, I would like to thank you for the two fulsome briefings that were provided by Postal Service officials to our Committee staff on October 22 and November 7, 2014, before this cyber-attack was made public. The information provided in these classified settings was helpful in conveying information about the potential attackers in this case and the possible scope of their destructive actions.

The increasing number of cyber-attacks in both the public and private sectors is unprecedented and poses a clear and present danger to our nation's security. For example, *USA Today* recently ran a front-page story reporting that 500 million records have been stolen from various financial institutions as a result of cyber-attacks over the past year, according to federal law enforcement officials. The report stated:

> Federal officials warned companies Monday that hackers have stolen more than 500 million financial records over the past 12 months, essentially breaking into banks without ever entering a building.[1]

The report also explained that law enforcement officials believe the "U.S. financial sector is one of the most targeted in the world."[2]

---

[1] *Officials Warn 500 Million Financial Records Hacked*, USA Today (Oct. 21, 2014) (online at www.usatoday.com/story/news/politics/2014/10/20/secret-service-fbi-hack-cybersecuurity/17615029/).

[2] *Id.*

Large companies such as Home Depot, Target, K-Mart, and Community Health Partners—one of the nation's largest hospital chains—have also been the victims of cyber-attacks in the past year.[3]

Federal contractors have also been targeted, including USIS, the nation's largest private provider of federal background investigations. USIS's network was penetrated in August, compromising the personal information of tens of thousands of federal employees. During a hearing before our Committee in September, the director of the U.S. Computer Emergency Readiness Team testified that malware attacks are "very frequent" and "happen every day across the globe on the Internet."[4]

The increased frequency and sophistication of cyber-attacks upon both public and private entities highlights the need for greater collaboration to improve data security. The Postal Service's knowledge, information, and experience in combating data breaches will be helpful as Congress examines federal cybersecurity laws and any necessary improvements to protect sensitive consumer and government financial information.

For these reasons, I request that the Postal Service provide the following information:

(1) a description of the cyber-attack, including the date and the manner in which it was first discovered, the dates the attack is believed to have begun and ended, and the actions you took after learning of this attack;

(2) the types of data breached, the number of employees and customers potentially affected, the manner in which employees and customers were notified of the breach, and the scope of any fraudulent transactions that resulted from the breach;

(3) the findings from forensic investigative analyses or reports concerning the breaches, including findings about vulnerabilities to malware, the use of data segmentation to protect Personally Identifiable Information (PII), and why the breach went undetected for the length of time it did;

---

[3] *Home Depot Data Breach Could Be the Largest Yet*, New York Times (Sept. 8, 2014) (online at http://bits.blogs.nytimes.com/2014/09/08/home-depot-confirms-that-it-was-hacked/?_php=true&_type=blogs&_r=0); *Target Cyber Breach Hits 40 Million Payment Cards at Holiday Peak*, Reuters (Dec. 19, 2013) (online at http://www.reuters.com/article/2013/12/19/us-target-breach-idUSBRE9BH1GX20131219); Kmart, *Kmart Investigating Payment System Intrusion* (Oct. 10, 2014) (online at http://www.kmart.com/ue/home/10.10.14_News_Release.pdf.); *Hack of Community Health Systems Affects 4.5 Million Patients*, New York Times (Aug. 18, 2014) (online at http://bits.blogs.nytimes.com/2014/08/18/hack-of-community-health-systems-affects-4-5-million-patients).

[4] House Committee on Oversight and Government Reform, *Hearing on Examining Obamacare's Failures in Security, Accountability, and Transparency* (Sept. 18, 2014).

(4) a description of data protection improvement measures the Postal Service has undertaken since discovering the breaches;

(5) a description of the data security policies and procedures that govern your relationships with vendors, third-party service providers, and subcontractors, including the manner by which you ensure that entities performing work on your behalf have reasonable data security controls in place to thwart cyber-attacks; and

(6) any recommendations for improvements in cybersecurity laws or the coordination of efforts to identify and respond to emerging trends in cybersecurity risks to help prevent future data breaches.

Please provide the requested information by December 19, 2014. If you have any questions about this request, please contact Timothy D. Lynch at (202) 225-0312.

Sincerely,

Elijah E. Cummings
Ranking Member

cc: The Honorable Darrell E. Issa, Chairman