

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

JOHN L. MICA, FLORIDA
MICHAEL R. TURNER, OHIO
JOHN J. DUNCAN, JR., TENNESSEE
PATRICK T. MCENRY, NORTH CAROLINA
JIM JORDAN, OHIO
JASON CHAFFETZ, UTAH
TIM WALBERG, MICHIGAN
JAMES LANKFORD, OKLAHOMA
JUSTIN AMASH, MICHIGAN
PAUL A. GOSAR, ARIZONA
PATRICK MEEHAN, PENNSYLVANIA
SCOTT DESJARLAIS, TENNESSEE
TREY GOWDY, SOUTH CAROLINA
BLAKE FARENTHOLD, TEXAS
DOC HASTINGS, WASHINGTON
CYNTHIA M. LUMMIS, WYOMING
ROB WOODALL, GEORGIA
THOMAS MASSIE, KENTUCKY
DOUG COLLINS, GEORGIA
MARK MEADOWS, NORTH CAROLINA
KERRY L. BENTIVOLIO, MICHIGAN
RON DESANTIS, FLORIDA

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) 225-6051
<http://oversight.house.gov>

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
STEPHEN F. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
JACKIE SPEIER, CALIFORNIA
MATTHEW A. CARTWRIGHT, PENNSYLVANIA
L. TAMMY DUCKWORTH, ILLINOIS
ROBIN L. KELLY, ILLINOIS
DANNY K. DAVIS, ILLINOIS
PETER WELCH, VERMONT
TONY CARDENAS, CALIFORNIA
STEVEN A. HORSFORD, NEVADA
MICHELLE LUJAN GRISHAM, NEW MEXICO
VACANCY

LAWRENCE J. BRADY
STAFF DIRECTOR

December 23, 2014

Michael Lynton
Chairman and CEO
Sony Pictures Entertainment, Inc.
10202 Washington Blvd.
Culver City, CA 90232

Dear Mr. Lynton:

I am writing to request information about a devastating cyber attack that was recently reported by Sony Pictures Entertainment. The attack caused significant disruption to Sony's computer systems beginning on November 24, 2014.¹ Reports indicate that in addition to deploying destructive malware, the attackers stole vast quantities of sensitive proprietary information, including soon-to-be-released films and the personal information of over 47,000 current and former employees, including their social security numbers and healthcare records.² The size, scope, and scale of the hack into Sony's systems "may be the most damaging cyberattack ever inflicted on an American business."³

The cyber attack is even more notable for the threats of violence that accompanied it. On December 16, 2014, the hackers who claimed responsibility for the attack, the "Guardians of Peace," sent emails threatening violence against movie theatres that intended to show the film "The Interview."⁴ The hackers invoked the attacks of September 11, 2001, and reportedly

¹ Sony Pictures, *Message For Current And Former Sony Pictures Employees And Dependents, And For Production Employees* (Dec. 15, 2014) (online at www.sonypictures.com/corp/notification/SPE_Cyber_Notification.pdf?#zoom=100).

² *Sony Breach May Have Exposed Employee Healthcare, Salary Data*, KrebsOnSecurity.com (Dec. 2, 2014) (online at <http://krebsonsecurity.com/2014/12/sony-breach-may-have-exposed-employee-healthcare-salary-data/>); *Sony Hack Exposed Personal Data of Hollywood Stars*, Wall Street Journal (Dec. 5, 2014) (online at www.wsj.com/articles/sony-pictures-hack-reveals-more-data-than-previously-believed-1417734425).

³ *Sony Cyberattack May Be Costliest Ever*, U.S. News and World Report (Dec. 18, 2014) (online at www.usnews.com/news/business/articles/2014/12/17/n-korea-linked-sony-hack-may-be-costliest-ever).

⁴ *Sony Hackers Reference 9/11 In New Threats Against Theatres*, Washington Post (Dec. 16, 2014) (online at www.washingtonpost.com/business/technology/sony-hackers-make-threats-in-first-phase-of-new-leaks/2014/12/16/1a15acf6-8553-11e4-abcf-5a3d7b3b20b8_story.html).

“urged people to leave their homes if located near theaters showing the film.”⁵ In response, Sony announced that it would not release the film as scheduled on Christmas Day.⁶ The company’s counsel subsequently indicated that it may seek to distribute the film in some form at a later date.⁷

This past Friday, FBI officials announced that they believe North Korea was behind this attack. The FBI indicated that “the tools used in the attack have similarities to a cyber attack in March of last year against South Korean banks and media outlets, which was carried out by North Korea.”⁸

The increasing number and sophistication of cyber attacks on both public and private entities pose a clear and present danger to our national security and highlight the urgent need for greater collaboration to improve data security. Sony’s knowledge, information, and experience will be helpful as Congress examines federal cybersecurity laws and any necessary improvements to protect sensitive consumer and government financial information. To aid in this oversight, I request that Sony provide the following information:

- (1) a description of all data breaches the company has experienced over the past year, including the date and the manner and method by which it first discovered the breaches, the dates the breaches are believed to have begun and ended, and the types of data breached;
- (2) the approximate number of current and former employees, as well as any customers that may have been affected by the breaches, and the manner in which current and former employees, as well as any customers were notified of the breaches;
- (3) the findings from any forensic investigative analyses or reports concerning the breaches, including findings about vulnerabilities to malware, the use of data segmentation to protect personally identifiable information, and why the breaches went undetected for the length of time they did;
- (4) a description of data protection improvement measures the company has undertaken since discovering the breaches;
- (5) a description of the data security policies and procedures that govern the company’s relationships with vendors, third-party service providers, and

⁵ *Id.*

⁶ *Sony Drops ‘The Interview’ Following Terrorist Threats*, New York Times (Dec. 17, 2014) (online at www.nytimes.com/2014/12/18/business/sony-the-interview-threats.html?_r=0).

⁷ *Sony Lawyer David Boies Says “The Interview” Will Be Distributed*, CBS News (Dec. 22, 2014) (online at www.cbsnews.com/news/sony-lawyer-david-boies-says-the-interview-will-be-released/).

⁸ Federal Bureau of Investigation, *Update on Sony Investigation* (Dec. 19, 2014).

Mr. Michael Lynton

Page 3

subcontractors, including the manner by which the company ensures that entities performing work on the company's 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 January 23, 2015. I also request a briefing from your Chief Information Security Officer or similar chief IT security professional by January 19, 2015. If you have any questions about this request, please contact Timothy D. Lynch at (202) 225-0312. Thank you for your cooperation in this matter.

Sincerely,



Elijah E. Cummings
Ranking Member

cc: The Honorable Darrell E. Issa, Chairman