



November 21, 2023

MR. JOHN R. GREENEWALD JR.
SUITE 1203
27305 WEST LIVE OAK ROAD
CASTAIC, CA 91384

FOIPA Request No.: 1355208-000
Subject: Director Comey's emails containing the word Wikileaks

Dear Mr. Greenewald:

The FBI has completed its review of records subject to the Freedom of Information/Privacy Acts (FOIPA) that are responsive to your request. The enclosed documents were reviewed under the FOIPA, Title 5, United States Code, Section 552/552a. Below you will find check boxes under the appropriate statute headings which indicate the types of exemptions asserted to protect information which is exempt from disclosure. The appropriate exemptions are noted on the enclosed pages next to redacted information. In addition, a deleted page information sheet was inserted to indicate where pages were withheld entirely and identify which exemptions were applied. The checked exemption boxes used to withhold information are further explained in the enclosed Explanation of Exemptions.

| Section 552 | | Section 552a |
|--|---|---------------------------------|
| <input checked="" type="checkbox"/> (b)(1) | <input type="checkbox"/> (b)(7)(A) | <input type="checkbox"/> (d)(5) |
| <input type="checkbox"/> (b)(2) | <input type="checkbox"/> (b)(7)(B) | <input type="checkbox"/> (j)(2) |
| <input checked="" type="checkbox"/> (b)(3) | <input checked="" type="checkbox"/> (b)(7)(C) | <input type="checkbox"/> (k)(1) |
| <u>18 U.S.C. § 3509(d)</u> | <input checked="" type="checkbox"/> (b)(7)(D) | <input type="checkbox"/> (k)(2) |
| <u>50 U.S.C. § 3024(i)(1)</u> | <input checked="" type="checkbox"/> (b)(7)(E) | <input type="checkbox"/> (k)(3) |
| <hr/> | <input type="checkbox"/> (b)(7)(F) | <input type="checkbox"/> (k)(4) |
| <input type="checkbox"/> (b)(4) | <input type="checkbox"/> (b)(8) | <input type="checkbox"/> (k)(5) |
| <input checked="" type="checkbox"/> (b)(5) | <input type="checkbox"/> (b)(9) | <input type="checkbox"/> (k)(6) |
| <input checked="" type="checkbox"/> (b)(6) | | <input type="checkbox"/> (k)(7) |

160 pages were reviewed and 17 pages are being released.

Please see the paragraphs below for relevant information specific to your request as well as the enclosed FBI FOIPA Addendum for standard responses applicable to all requests.

Based on the information you provided, we conducted a search of the places reasonably expected to have records. For more information about records searches and the standard search policy, see the enclosed FBI FOIPA Addendum General Information Section.

In response to your narrowed/negotiated Freedom of Information/Privacy Acts (FOIPA) request, enclosed are the processed documents.

This is the final release of information responsive to your FOIPA request. This material is being provided to you at no charge.

Please refer to the enclosed FBI FOIPA Addendum for additional standard responses applicable to your request. “Part 1” of the Addendum includes standard responses that apply to all requests. “Part 2” includes additional standard responses that apply to all requests for records about yourself or any third party individuals. “Part 3” includes general information about FBI records that you may find useful. Also enclosed is our Explanation of Exemptions.

Additional information about the FOIPA can be found at www.fbi.gov/foia. Should you have questions regarding your request, please feel free to contact foipaquestions@fbi.gov. Please reference the FOIPA Request number listed above in all correspondence concerning your request.

If you are not satisfied with the Federal Bureau of Investigation’s determination in response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, 441 G Street, NW, 6th Floor, Washington, D.C. 20530, or you may submit an appeal through OIP’s FOIA STAR portal by creating an account following the instructions on OIP’s website: <https://www.justice.gov/oip/submit-and-track-request-or-appeal>. Your appeal must be postmarked or electronically transmitted within ninety (90) days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." Please cite the FOIPA Request Number assigned to your request so it may be easily identified.

You may seek dispute resolution services by emailing the FBI’s FOIA Public Liaison at foipaquestions@fbi.gov. The subject heading should clearly state “Dispute Resolution Services.” Please also cite the FOIPA Request Number assigned to your request so it may be easily identified. You may also contact the Office of Government Information Services (OGIS). The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

Sincerely,



Michael G. Seidel
Section Chief
Record/Information Dissemination Section
Information Management Division

Enclosures

FBI FOIPA Addendum

As referenced in our letter responding to your Freedom of Information/Privacy Acts (FOIPA) request, the FBI FOIPA Addendum provides information applicable to your request. Part 1 of the Addendum includes standard responses that apply to all requests. Part 2 includes standard responses that apply to requests for records about individuals to the extent your request seeks the listed information. Part 3 includes general information about FBI records, searches, and programs.

Part 1: The standard responses below apply to all requests:

- (i) **5 U.S.C. § 552(c).** Congress excluded three categories of law enforcement and national security records from the requirements of the FOIPA [5 U.S.C. § 552(c)]. FBI responses are limited to those records subject to the requirements of the FOIPA. Additional information about the FBI and the FOIPA can be found on the www.fbi.gov/foia website.
- (ii) **Intelligence Records.** To the extent your request seeks records of intelligence sources, methods, or activities, the FBI can neither confirm nor deny the existence of records pursuant to FOIA exemptions (b)(1), (b)(3), and as applicable to requests for records about individuals, PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(1), (b)(3), and (j)(2)]. The mere acknowledgment of the existence or nonexistence of such records is itself a classified fact protected by FOIA exemption (b)(1) and/or would reveal intelligence sources, methods, or activities protected by exemption (b)(3) [50 USC § 3024(i)(1)]. This is a standard response and should not be read to indicate that any such records do or do not exist.

Part 2: The standard responses below apply to all requests for records on individuals:

- (i) **Requests for Records about any Individual—Watch Lists.** The FBI can neither confirm nor deny the existence of any individual's name on a watch list pursuant to FOIA exemption (b)(7)(E) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (j)(2)]. This is a standard response and should not be read to indicate that watch list records do or do not exist.
- (ii) **Requests for Records about any Individual—Witness Security Program Records.** The FBI can neither confirm nor deny the existence of records which could identify any participant in the Witness Security Program pursuant to FOIA exemption (b)(3) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(3), 18 U.S.C. 3521, and (j)(2)]. This is a standard response and should not be read to indicate that such records do or do not exist.
- (iii) **Requests for Confidential Informant Records.** The FBI can neither confirm nor deny the existence of confidential informant records pursuant to FOIA exemptions (b)(7)(D), (b)(7)(E), and (b)(7)(F) [5 U.S.C. § 552 (b)(7)(D), (b)(7)(E), and (b)(7)(F)] and Privacy Act exemption (j)(2) [5 U.S.C. § 552a (j)(2)]. The mere acknowledgment of the existence or nonexistence of such records would reveal confidential informant identities and information, expose law enforcement techniques, and endanger the life or physical safety of individuals. This is a standard response and should not be read to indicate that such records do or do not exist.

Part 3: General Information:

- (i) **Record Searches and Standard Search Policy.** The Record/Information Dissemination Section (RIDS) searches for reasonably described records by searching systems, such as the Central Records System (CRS), or locations where responsive records would reasonably be found. The CRS is an extensive system of records consisting of applicant, investigative, intelligence, personnel, administrative, and general files compiled by the FBI per its law enforcement, intelligence, and administrative functions. The CRS spans the entire FBI organization, comprising records of FBI Headquarters, FBI Field Offices, and FBI Legal Attaché Offices (Legats) worldwide; Electronic Surveillance (ELSUR) records are included in the CRS. The standard search policy is a search for main entity records in the CRS. Unless specifically requested, a standard search does not include a search for reference entity records, administrative records of previous FOIPA requests, or civil litigation files.
 - a. *Main Entity Records* – created for individuals or non-individuals who are the subjects or the focus of an investigation
 - b. *Reference Entity Records*- created for individuals or non-individuals who are associated with a case but are not known subjects or the focus of an investigation
- (ii) **FBI Records.** Founded in 1908, the FBI carries out a dual law enforcement and national security mission. As part of this dual mission, the FBI creates and maintains records on various subjects; however, the FBI does not maintain records on every person, subject, or entity.
- (iii) **Foreseeable Harm Standard.** As amended in 2016, the Freedom of Information Act provides that a federal agency may withhold responsive records only if: (1) the agency reasonably foresees that disclosure would harm an interest protected by one of the nine exemptions that FOIA enumerates, or (2) disclosure is prohibited by law (5 United States Code, Section 552(a)(8)(A)(i)). The FBI considers this foreseeable harm standard in the processing of its requests.
- (iv) **Requests for Criminal History Records or Rap Sheets.** The Criminal Justice Information Services (CJIS) Division provides Identity History Summary Checks – often referred to as a criminal history record or rap sheet. These criminal history records are not the same as material in an investigative “FBI file.” An Identity History Summary Check is a listing of information taken from fingerprint cards and documents submitted to the FBI in connection with arrests, federal employment, naturalization, or military service. For a fee, individuals can request a copy of their Identity History Summary Check. Forms and directions can be accessed at www.fbi.gov/about-us/cjis/identity-history-summary-checks. Additionally, requests can be submitted electronically at www.edo.cjis.gov. For additional information, please contact CJIS directly at (304) 625-5590.

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552


- (b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;
- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
- (k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
- (k)(4) required by statute to be maintained and used solely as statistical records;
- (k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
- (k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

This document is made available through the declassification efforts
and research of John Greenewald, Jr., creator of:

The Black Vault



The Black Vault is the largest online Freedom of Information Act (FOIA) document clearinghouse in the world. The research efforts here are responsible for the declassification of hundreds of thousands of pages released by the U.S. Government & Military.

Discover the Truth at: <http://www.theblackvault.com>

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1355208-000

Total Deleted Page(s) = 143
Page 2 ~ b1; b3; b6; b7C; b7E;
Page 3 ~ b6; b7C; b7E;
Page 4 ~ b1; b3; b6; b7C; b7E;
Page 5 ~ b1; b3; b6; b7C; b7E;
Page 6 ~ b1; b3; b6; b7C; b7E;
Page 7 ~ b1; b3; b6; b7C; b7D; b7E;
Page 8 ~ b1; b3; b6; b7C; b7E;
Page 9 ~ b1; b3; b6; b7C; b7E;
Page 10 ~ b1; b3; b6; b7C; b7E;
Page 11 ~ b1; b3; b6; b7C; b7E;
Page 12 ~ b1; b3; b6; b7C; b7E;
Page 13 ~ b6; b7C; b7E;
Page 14 ~ b6; b7C; b7E;
Page 15 ~ b6; b7C; b7E;
Page 16 ~ b6; b7C; b7E;
Page 17 ~ b7E;
Page 18 ~ b7E;
Page 19 ~ b6; b7C; b7E;
Page 20 ~ b7E;
Page 21 ~ b7E;
Page 22 ~ b7E;
Page 23 ~ b7E;
Page 24 ~ b6; b7C; b7E;
Page 25 ~ b6; b7C; b7E;
Page 26 ~ b3; b7E;
Page 27 ~ b6; b7C; b7E;
Page 28 ~ b6; b7C; b7E;
Page 29 ~ b6; b7C; b7E;
Page 30 ~ b6; b7C; b7E;
Page 31 ~ b7E;
Page 32 ~ b7E;
Page 33 ~ b6; b7C; b7E;
Page 34 ~ b7E;
Page 35 ~ b7E;
Page 36 ~ b6; b7C; b7E;
Page 37 ~ b7E;
Page 38 ~ b3; b7E;
Page 39 ~ b7E;
Page 40 ~ b7E;
Page 41 ~ b6; b7C; b7E;
Page 42 ~ b7E;
Page 43 ~ b6; b7C; b7E;
Page 44 ~ b6; b7C; b7E;
Page 45 ~ b6; b7C; b7E;
Page 46 ~ b7E;
Page 47 ~ b7E;
Page 48 ~ b6; b7C; b7E;
Page 49 ~ b7E;
Page 50 ~ b7E;
Page 51 ~ b6; b7C; b7E;
Page 52 ~ b7E;
Page 53 ~ b6; b7C; b7E;
Page 54 ~ b7E;
Page 55 ~ b5; b7E;
Page 56 ~ b5; b6; b7C; b7E;
Page 57 ~ b5; b7E;
Page 58 ~ b6; b7C; b7E;
Page 59 ~ b7E;
Page 60 ~ b5; b6; b7C; b7E;
Page 61 ~ b1; b3; b6; b7C; b7E;
Page 62 ~ b6; b7C; b7E;
Page 63 ~ b1; b3; b6; b7C; b7E;
Page 64 ~ b1; b3; b6; b7C; b7D; b7E;
Page 65 ~ b1; b3; b7E;
Page 66 ~ b1; b3; b6; b7C; b7E;
Page 67 ~ b1; b3; b6; b7C; b7E;
Page 68 ~ b1; b3; b6; b7C; b7E;

Page 69 ~ b1; b3; b6; b7C; b7E;
Page 70 ~ b1; b3; b6; b7C; b7E;
Page 71 ~ b1; b3; b6; b7C; b7D; b7E;
Page 72 ~ b1; b3; b6; b7C; b7E;
Page 73 ~ b1; b3; b6; b7C; b7E;
Page 74 ~ b1; b3; b6; b7C; b7E;
Page 75 ~ b7E;
Page 76 ~ b7E;
Page 77 ~ b3; b7E;
Page 78 ~ b7E;
Page 79 ~ b3; b6; b7C; b7E;
Page 80 ~ b6; b7C; b7E;
Page 81 ~ b6; b7C; b7E;
Page 82 ~ b3; b6; b7C; b7E;
Page 83 ~ b6; b7C; b7E;
Page 84 ~ b7E;
Page 85 ~ b7E;
Page 86 ~ b7E;
Page 87 ~ b6; b7C; b7E;
Page 88 ~ b7E;
Page 89 ~ b7E;
Page 90 ~ b7E;
Page 91 ~ b6; b7C; b7E;
Page 92 ~ b7E;
Page 93 ~ b7E;
Page 94 ~ b6; b7C; b7E;
Page 95 ~ b6; b7C; b7E;
Page 96 ~ b6; b7C; b7E;
Page 97 ~ b6; b7C; b7E;
Page 98 ~ b7E;
Page 99 ~ b1; b3; b6; b7C; b7E;
Page 100 ~ b3; b6; b7C; b7E;
Page 101 ~ b7E;
Page 102 ~ b7E;
Page 103 ~ b7E;
Page 104 ~ b6; b7C; b7E;
Page 105 ~ b7E;
Page 106 ~ b7E;
Page 107 ~ b6; b7C; b7E;
Page 108 ~ b7E;
Page 109 ~ b7E;
Page 110 ~ b6; b7C; b7E;
Page 111 ~ b7E;
Page 112 ~ b6; b7C; b7E;
Page 113 ~ b7E;
Page 114 ~ b7E;
Page 115 ~ b7E;
Page 116 ~ b7E;
Page 117 ~ b7E;
Page 118 ~ b6; b7C; b7D; b7E;
Page 119 ~ b7E;
Page 120 ~ b3; b7E;
Page 121 ~ b7E;
Page 122 ~ b7E;
Page 123 ~ b7E;
Page 124 ~ b7E;
Page 125 ~ b6; b7C; b7E;
Page 126 ~ b7E;
Page 127 ~ b6; b7C; b7E;
Page 128 ~ b6; b7C; b7E;
Page 129 ~ b6; b7C; b7E;
Page 130 ~ b7E;
Page 131 ~ b7E;
Page 132 ~ b7E;
Page 133 ~ b7E;
Page 134 ~ b6; b7C; b7E;
Page 135 ~ b6; b7C; b7E;
Page 136 ~ b7E;
Page 137 ~ b7E;
Page 138 ~ b7E;
Page 139 ~ b7E;
Page 140 ~ b7E;
Page 141 ~ b7E;

Page 142 ~ b7E;
Page 143 ~ b7E;
Page 144 ~ b7E;

XXXXXXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXXXXXX

[redacted]

From: [redacted]
Sent: Friday, January 23, 2015 11:25 AM
To: COMEY, JAMES B. (DO) (FBI)
Cc: [redacted]
Subject: Weekend Book --- ~~SECRET~~
Attachments: Director Final_23Jan-15.pdf

Classification: ~~SECRET~~

~~Classified By: [redacted]
Derived From: FBI NSIC, dated 20120629
Declassify On: 20401231~~

=====

=====
Classification: ~~SECRET~~

[Redacted]

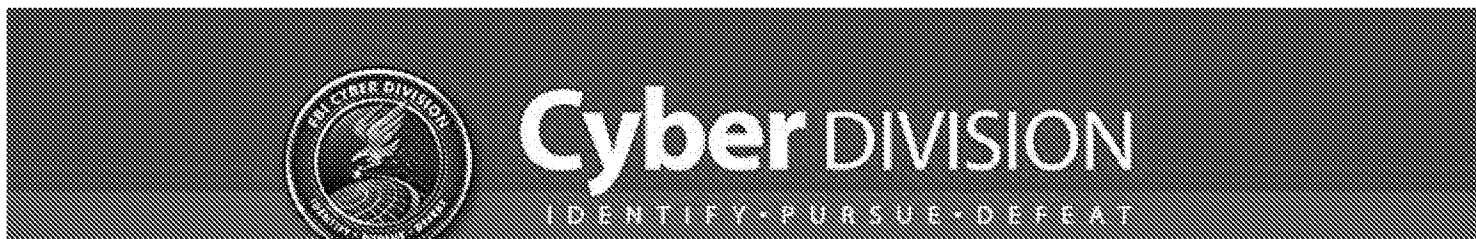
b6
b7C
b7E

From: [Redacted]
Sent: Tuesday, August 18, 2015 12:58 PM
To: COMEY, JAMES B. (DO) (FBI)
Subject: FW: Sony article in Harvard Business Review --- UNCLASSIFIED
Attachments: HBR_Sony_interview.pdf

Classification: UNCLASSIFIED
=====

From: [Redacted]
Sent: Monday, August 17, 2015 11:44 AM
Subject: Sony article in Harvard Business Review --- UNCLASSIFIED

Classification: UNCLASSIFIED
=====



Please see attached for an article which may be of interest to you. *Harvard Business Review* just ran the attached interview with Sony Pictures Entertainment [Redacted] regarding the attack on Sony's networks. Not only is the piece interesting, [Redacted] b6 [Redacted] has some very positive things to say about the FBI's involvement in the investigation. Notably, when asked what advice b7C he would offer other executives caught up in a hacking crisis, he says, "... it's important to bring the FBI in early. Some companies are reluctant to do so; I think that's a mistake."

Kudos to each of you, whether involved in this case or not, who work every day to protect the great reputation of the FBI and the Cyber Division!

FBI Cyber Division Executive Staff Unit

[Redacted]

b7E

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

THE HBR INTERVIEW





“They Burned the House Down”

MICHAEL LYNTON'S "BLACK SWAN" materialized late last year, when someone—the U.S. government says it was North Korea—pulled off the most devastating hack in corporate history. Lynton, the CEO of Sony Pictures Entertainment, had to look on as highly confidential company information—salary details, private e-mails (some of them harshly critical of top Hollywood talent), unreleased movies—was leaked for all the world to see. For good measure, the hackers wiped out huge amounts of data on the company's servers.

The attack pushed a reluctant Lynton to the forefront of U.S. foreign relations when the

“THEY BURNED THE HOUSE DOWN”

hackers threatened retaliation if *The Interview*, a Sony Pictures comedy set in North Korea that includes the assassination of Kim Jong-un, was released. Fearing reprisals, many theaters declined to screen the film, and Sony had to look for alternative distribution. President Barack Obama weighed in, chastising Sony for what he viewed as caving to Pyongyang’s pressure. The R-rated bro film had suddenly become a First Amendment icon.

How does an institution make it through all that? How does it sustain its culture, and retain its talent, as each salacious, embarrassing, top-secret bit of information spills out into public? I visited Lynton in his sumptuous office at Sony Pictures’ fabled art deco complex in Culver City, California, to talk about the experience. He seemed unguarded and optimistic, freely acknowledging the difficulties Sony faced in the weeks after the attack, yet sounding hopeful that the company had made it through intact.

Attacks like this may well be the new normal. Lynton says he can only hope that his company’s nightmare will serve as a wake-up call for other U.S. businesses.

—Adi Ignatius

Let’s go back to the end of last year. Sony had just been hacked. What were your first thoughts?

I was on my way to work. It was about 8:00 in the morning, and our CFO called to say that we had been breached. By the time I got to the office, the whole studio was off-line.

And that was just the beginning. Yes. We received a series of threatening messages warning of a data dump of the information the hackers had stolen, and then the disclosures began. Soon we were dealing with a few things at once. We were trying to keep the business operating. We were dealing with employees who feared their information would be made public. We were dealing with the press, which was publishing some of the e-mails. And then we had the FBI coming in to do forensic analysis.

You were known as a CEO who tended to delegate. Did that change? Yes, my role changed radically and quickly. The crisis required me to be very hands-on. We set up a command central to ensure that all decisions were made with my understanding and knowledge and approval. That basically became a full-time job, which meant everybody

else had to operate the business—which they did, very successfully.

What went into setting up the command central?

The first thing was to establish a means of communication in the absence of e-mail. We were basically analog for a while. We had phones, and that was it. So we set up texting trees and then turned to our employee notification system. That meant we could centrally text our employee population, which we did frequently.

Was this just for crisis-related communications, or to sustain business as usual?

It was for business as usual, making sure people could communicate with one another about the stuff we do on a daily basis—making movies, making television shows, ensuring that everything gets distributed. Then we needed to create a temporary e-mail system. And we had to set up systems to make payroll, pay vendors, and so on. Making payroll alone was a monumental task: The finance department hauled old machines out of the basement to cut checks.

It sounds like a nightmare. I can’t imagine seeing all my personal information suddenly made public.

Well, that was just part of it. The bigger challenge was that the folks who did this didn’t just steal practically everything from the house; they burned the house down. They took our data. Then they wiped stuff off our computers. And then they destroyed our servers and our computers.

So they had it, and you didn’t. Correct. We had backup, but we couldn’t access it until we had computers, servers, and systems that would allow us to do so. So you have these very public e-mails out there, some of which are salacious. And then you have the challenge of operating the business when the networked services you’ve relied on are unavailable.

Containing the Damage

What did your employees need most from you at that point? They needed reassurance. They were concerned that their personal information was out there and available, and we had to explain exactly what we were doing to protect them. Some were afraid that the company might go under as a result of all this.

Nightmarish Days: A Timeline of the 2014 Sony Hack

| WEEK 1 | WEEK 2 | WEEK 3 | WEEK 4 | WEEK 5 | WEEK 6 | WEEK 7 | WEEK 8 | WEEK 9 | WEEK 10 | WEEK 11 |
|--|--|---|--|--|--|--------|--------|--------|---------|---------|
| <p>● NOVEMBER 24 When Sony Pictures Entertainment (SPE) employees log on to their computers, they see a skeleton and the words “Hacked by the #GOP” (Guardians of Peace). The hackers steal confidential business information, including employee data and private e-mails, and movies, including <i>Annie</i> and other unreleased films.</p> <p>● NOVEMBER 25 SPE’s top two executives, Michael Lynton and Amy Pascal, first communicate with employees to commend their hard work while the company strives to resolve the system disruption.</p> | <p>● DECEMBER 2 Lynton and Pascal e-mail employees acknowledging that a brazen attack has occurred and stating that SPE is working closely with law enforcement officials.</p> <p>● DECEMBER 5 Certain SPE employees receive an e-mail from someone claiming to be a GOP member, demanding that they disassociate themselves from Sony, and threatening, “If you don’t, not only you but your family will be in danger.”</p> <p>● DECEMBER 5 Lynton forwards an e-mail from the cybersecurity expert Kevin Mandia to all employees to explain the nature of the attack: “This was an unparalleled and well-planned crime, carried out by an organized group, for which neither SPE nor other companies could have been fully prepared.”</p> <p>● DECEMBER 7 The Korean Central News Agency describes the attack as a “righteous deed” but dismisses reports of North Korean involvement as a “wild rumor.”</p> <p>● DECEMBER 8 The GOP posts a message demanding that the studio “stop immediately showing the movie of terrorism which can break the regional peace and cause the War” and linking to sensitive information stolen from SPE.</p> | <p>● DECEMBER 11 Pascal issues an apology after her personal e-mails are made public. Sony stages a quiet Los Angeles premiere for <i>The Interview</i>.</p> <p>● DECEMBER 14 David Boies, outside counsel for SPE, writes to journalists reminding them that the leaked material is “stolen information” and calls on media outlets not to read or publish any SPE documents in their possession.</p> <p>● DECEMBER 15 Lynton calls an “all hands” meeting to tell employees they “should not be worried about the future of this studio.”</p> <p>● DECEMBER 15-16 Two separate class-action lawsuits are filed on behalf of former and current employees alleging that Sony did not do enough to safeguard their private information.</p> <p>● DECEMBER 16 The GOP posts a 9/11-type threat against moviegoers who try to see <i>The Interview</i> when it’s released on Christmas Day. Major theater chains start to cancel screenings.</p> | <p>● DECEMBER 17 SPE decides not to move forward with the movie’s planned nationwide theatrical release the following week.</p> <p>Lynton and SPE executives begin reaching out to potential digital distribution partners, including Google.</p> <p>● DECEMBER 18 The FBI publicly states that North Korea was behind the attack. President Obama, too, attributes the attack to North Korea.</p> <p>Obama calls canceling the theatrical release “a mistake” and adds, “They should have called me.”</p> <p>● DECEMBER 22 North Korea experiences a 10-hour internet outage; connectivity problems continue for days.</p> <p>● DECEMBER 23 SPE announces that <i>The Interview</i> will have a limited theatrical release on Christmas Day.</p> <p>● DECEMBER 24 <i>The Interview</i> is released on Google Play, YouTube Movies, Microsoft’s Xbox Video, and a dedicated site run by the studio through Kernel and Stripe.</p> | <p>● JANUARY 20 SPE announces that <i>The Interview</i> was rented or bought online and through cable, satellite, and telecom providers more than 5.8 million times, for a total of some \$40 million in consumer sales, and that the movie has made \$6 million in box office receipts through its limited theatrical release.</p> | <p>● FEBRUARY 4 SPE says the hack cost \$15 million through the end of 2014.</p> <p>● FEBRUARY 5 Pascal resigns.</p> | | | | | |

How did you reach out to them? We held big town hall meetings, with 3,000 to 4,000 people at a time, to talk about what was happening. And we held small forums, where we brought together groups of 50 to 80 and listened to their concerns. I usually ate by myself in the cafeteria and made sure people could just come up and speak with me. Physical presence was very important. I left in the middle of all this to go to Japan for about a day and a half, because I had to make a board presentation on our budget. When I got back, our head of HR, George Rose, said, “Why have you been gone so long?” And I said, “George, I’ve been gone *36 hours*.” Time felt very compressed, because things were happening so quickly.

Were your employees also angry? Some were, yes. And once they heard that the U.S. government thought the hack was done by North Korea, some were angry that we were releasing *The Interview*. When you take a job in a movie studio, this is not what you think you’re signing up for.

How did you cope with the exposure of so much private material? It was complicated, for a couple of reasons. There was the celebrity-related stuff people were reading in the newspapers, which was distracting to employees, especially those whose e-mails were being published. And then there was the fact that employees could look up one another’s e-mails and read them.

Was there any way to contain that? We encouraged people not to rubberneck—meaning “Don’t go and look at the e-mails.”

What could you do about the e-mails that went public? Nothing, other than try to turn a blind eye and say that it was a distraction that needed to be treated as just that.

How did you survive the criticism of celebrities that was in the e-mails? In your business, you’re dealing with some of the biggest egos in the world. In some cases we had to pick up the phone and apologize. But for the most part, people shrugged it off. The Hollywood community, while close, is also transactional. People want to make movies and television shows. And frankly, I think a lot can be forgiven in that process.

“When you take a job in a movie studio, this is not what you think you’re signing up for.”

Have you lost any talent? No, we haven’t.

You did lose one senior colleague: Amy Pascal, who stepped down from her job as cochair. Was that necessary for the company to move forward—particularly since she had written some of the most troubling e-mails? No, that wasn’t the issue. Our mutual decision for her to move over to a producing role coincided with her contract’s coming due. It was time for a change in the motion picture group.

You won’t be the last company that’s breached. What are some lessons to impart from your experience? I think everybody is more cautious about what they put in e-mail, and the instinct nowadays is more often to pick up the phone or meet in person, particularly when you’re talking about difficult stuff.

Didn’t we already know not to put stuff in e-mail? Yes, but you say to yourself, *Ah, it’s never going to happen*. And I have to say that people’s short-term memories are unbelievably short. I’m receiving e-mails now that make me think as I read them, *Really?*



Have you looked at the leaked e-mails? I haven't. And they weren't leaked. They were stolen.

So the only content you know about personally is what blew up into media stories. Yes. I didn't even look at my own. And to pore through other people's e-mails would require thousands of hours. I didn't see the point of that.

Besides caution with e-mail, what are some take-aways from all this? There's the fundamental issue of what should or shouldn't be up on the network. The FBI said that 90% of companies would have been unable to withstand the attack. Nonetheless, everything that's up on the network is by definition susceptible to a breach. It's complicated, because ease of communication and access to data are part of what makes business operations run efficiently. But the more you have up there, the more vulnerable you are to hacking.

You even lost entire movies, right? The hackers stole a few movies that they released, including *Annie* and *Still Alice*. We believe they may also have stolen *The Interview*, but if they did, they chose not to release it.

To Release or Not to Release?

Do you accept the theory that North Korea did the hacking? I actually haven't been concerned about who did this. I've been more concerned about getting the business up and running and making sure folks here feel calm enough and secure enough to keep on with their jobs. What the FBI and others in the government have told me, and what the president of the United States has said, is that it was North Korea. I have to believe them. They did the forensics; they did the intelligence work.

As you know, some people think that's not true for a number of reasons, including the fact that the hackers said nothing about *The Interview* in their earliest communications. The U.S. government has access to more information about this than anyone else, and I have no reason to disagree. Experts have told me that the level of destruction and sophistication suggests it was a very expensive operation requiring a lot of people. I personally don't know whether it was the North Koreans or another entity, but I don't think it was some disgruntled employee. It was way too sophisticated.

“THEY BURNED THE HOUSE DOWN”

Given that it may have been North Korea, do you have any regrets about aspects of *The Interview*—such as that it identified Kim Jong-un and North Korea by name? No. Once you decide to go forward with making a movie, you’re under an obligation to yourself and the creative community to ensure that it gets out. We stayed true to that.

As a moviegoer, I was a bit bothered that *The Interview*—this sudden poster child for the First Amendment—wasn’t better. The whole affair seemed unlike the fatwa on Salman Rushdie. Well, have you read *The Satanic Verses*? It’s not *Midnight’s Children*. I mean, it wasn’t Rushdie’s greatest book. And I daresay the cartoons in Paris were not works of art. So the issue isn’t what you’re defending. It’s your obligation to defend. *The Interview* probably got a lot more scrutiny than it would have if we’d just put it out at Christmas as an R-rated comedy. Yes, I wish it were some great thing. It’s not a great work of art. But the examples I just described weren’t either.

You took a lot of heat when you initially postponed the movie’s theatrical release. That was a dark moment. And then President Obama spoke out, criticizing us. It wasn’t that we didn’t want to get the movie out but that theaters didn’t want to screen it. And we were already trying to line up digital distribution partners. But it’s not fun having the president wag his finger at your company.

How did you scramble to make things happen when it was clear you couldn’t have a normal theatrical release? I started calling people to ask if they would release it digitally. The majority said no. A lot of the e-commerce players and large cable operators and satellite operators were concerned about getting hacked themselves. For the first time, I thought, *We may not be able to get this out*. But then I spoke to Eric Schmidt, at Google, who said, “This is just the moment we’ve been waiting for. We think our security is up to this.” And Google helped get the film out on YouTube and Google Play.

Did anything useful come out of the patchwork distribution model that you put in place with Google and others? People often ask that, because there’s an ongoing debate in our industry about whether we should release movies digitally at the same time we release them theatrically. I still believe very strongly in the theatrical experience. And what happened here was one of a kind. We cobbled together an e-commerce site with a couple of small companies, Kernel and Stripe; we had Google and Microsoft involved; and others trickled in later.

Were there attempts to hack Google? I gather a lot of stuff was going on. But in the end, nothing bad came to Google, or Microsoft, or the others.

Does It Ever End?

Is the crisis over? Will it ever be over? I don’t want to jinx things, but I think it’s over. I hope so. Most of our systems have come back online. And I don’t think any revelations are still to come.

I read that the eventual cost to the company was \$15 million. The \$15 million Sony reported was the cost as of December 31. But the bottom line—and it’s a testament to the people here—is that we didn’t miss a single day’s start on a single television show or on a single movie.

WikiLeaks, meanwhile, is keeping the stolen data public and cataloging it for ease of search. I think Julian Assange’s argument is that Sony is a big, influential public company and thus these documents deserve to be publicly accessible. I take it you don’t agree. I don’t agree, particularly because there’s so much personal information in there. I think people have a right to their privacy. And

“This event was a relatively inexpensive, very noisy canary in the coal mine.”

anyway, the e-mails were stolen. For that matter, I don't agree with the way the press has been looking through the e-mails.

How much success did you have putting a halt to the press reports? Certain publications behaved honorably. They basically held back from doing a deep dive into the e-mails. Others didn't; they assigned large groups of reporters to go through the e-mails.

Were you surprised, or disappointed, by the lack of solidarity from others in your industry—that they didn't say, "We are all Sony"? I was surprised at first. But in retrospect I think our competitors were worried about getting hacked themselves, and worried about shareholder lawsuits if they came forward in support of us and then were hacked.

Did anything positive come out of this debacle? If you think about it, this event was a relatively inexpensive, very noisy canary in the coal mine for the United States. Imagine if it had happened to General Electric, and Jeff Immelt's e-mails were opened up. I have no idea what's in them, but I daresay they're not e-mails about big movie stars. The damage to an organization the size of GE would have been much greater than what happened here. So if there's a silver lining, it's that this was a call for America to wake up and pay attention. This is going to happen—in fact, it already is happening, on a regular basis.

Is your security better than it was before the hack? We're about to bring new systems online, which will have new protocols and security. But a lot of it, as I mentioned, is about what you put on the network. My wife made it obvious to me at one point, when she reminded me that she keeps her jewelry in a safe deposit box and takes it out only when she plans to wear it over a weekend. She doesn't leave it at home. That's how you have to view a network. You have to think carefully about what data needs to be up there.

Why are you willing to talk about this incident? For a number of reasons. First, I don't think people properly appreciate what the folks at Sony Pictures went through and what a spectacular job they did in keeping the company going. I also don't think people understand the level of destruction we

suffered. Coverage about the stolen e-mails did a lot to obscure what was really at stake here. When you get attacked like this, your entire business is in jeopardy.

The Voice of Experience

What other advice would you offer executives caught up in a hacking crisis like this? Staying calm is essential. And you need to be open and candid and constantly communicating. If you aren't, morale will suffer and people will leave. You also have to set priorities. The businesses we brought back first were the ones that generated revenue, even as other things fell by the wayside. Lastly, it's important to bring the FBI in early. Some companies are reluctant to do so; I think that's a mistake.

Have your personal priorities changed? This is going to sound naive, but the crisis demonstrated how overreliant we are on e-mail and the network. We should wean ourselves off it. Not that we have to walk around with abacuses, but nonetheless.

Has Sony Pictures managed to preserve its culture? You can't prepare for a black swan event. It just happens. But this did bring the place together. It forced everybody to work closely in a way that they hadn't in the past. And they liked that experience. I got to meet a lot of people I normally wouldn't meet and hear their concerns. We're trying to wrestle now with how to preserve all that.

What did this experience teach you about leadership? You have to be incredibly optimistic at all times about getting through a crisis—even if you're not quite sure how you're going to get through it. You need to be a thousand percent convinced in your own head, or you won't get across the finish line.

Isn't that just temperament? Aren't you just an optimistic person? I'm actually not very optimistic, for the most part. But in times of crisis I become unreasonably so.

You mean falsely optimistic? No, it's not about false optimism, because—and this will sound like bad movie dialogue—failure just isn't an option. You need to project a sort of cheerleading optimism, or you're not going to find your way. ▾

HBR Reprint R1507J

Harvard Business Review Notice of Use Restrictions, May 2009

Harvard Business Review and Harvard Business Publishing Newsletter content on EBSCOhost is licensed for the private individual use of authorized EBSCOhost users. It is not intended for use as assigned course material in academic institutions nor as corporate learning or training materials in businesses. Academic licensees may not use this content in electronic reserves, electronic course packs, persistent linking from syllabi or by any other means of incorporating the content into course resources. Business licensees may not host this content on learning management systems or use persistent linking or other means to incorporate the content into learning management systems. Harvard Business Publishing will be pleased to grant permission to make this content available through such means. For rates and permission, contact permissions@harvardbusiness.org.

[REDACTED]

From: [REDACTED]
Sent: Monday, July 25, 2016 4:48 PM
To: [REDACTED]
Subject: OPA Horizon 7/25/2016 --- UNCLASSIFIED//~~FOUO~~

Classification: UNCLASSIFIED//~~FOUO~~

=====

FBI Office of Public Affairs
The Horizon
Monday, July 25, 2016

National Issues

- DNC Emails: OPA - Received numerous media inquiries on the recent reporting of the Wikileaks release of DNC emails. OPA coordinated with the Cyber Division and released the following statement to media regulars: "The FBI is investigating a cyber intrusion involving the DNC and is working to determine the nature and scope of the matter. A compromise of this nature is something we take very seriously, and the FBI will continue to investigate and hold accountable those who pose a threat in cyberspace." The statement was attributed to the FBI as an organization.
- Brazil terrorism: OPA - Several news outlets asked if the FBI provided information to Brazil which led to arrests for possible plotting of attacks aimed at the Olympics. The reporters said Brazilian officials said the FBI provided such information. OPA referred reporters to Brazilian authorities who are investigating the matter.
- FBI.gov Top Story: OPA - The FBI's Weapons of Mass Destruction Directorate was established 10 years ago and today serves as a central hub for WMD subject-matter expertise.
<https://www.fbi.gov/news/stories/weapons-of-mass-destruction-directorate-marks-10-years>

Local Stories

- Chicago - FBI Chicago executed arrest warrants on 15 individuals charged with RICO violations. The operation targeted gang members in Chicago's western suburbs. The arrests were made by FBI Chicago SWAT Agents, neighboring FBI Division SWAT Teams, and an HRT team.
- Cleveland - Media coordinator continued to receive inquiries regarding FBI activity conducted last week during the RNC. Previously approved responses were provided
- Cleveland - Continued to receive inquiries regarding the abduction and murder of Sierha Jouglin. Media coordinator informed reporters the FBI is assisting the Fulton County Sheriff's Office, an investigation is ongoing and an individual is in custody.
- Detroit - Detroit Field Office top management and supervisors attended a leadership seminar at Michigan State University. Athletics Director Mark Hollis spoke about leadership and the value of publicly recognizing peers, the need for team-building exercises, the importance of communication, and how taking people out of their comfort zones can help build relationships.
- Miami - LATAM Airlines Group S.A., a commercial airline company based in Chile, has agreed to pay a \$12.75 million criminal penalty in connection with a scheme to pay bribes to Argentine union officials via a false consulting contract with a third-party intermediary in violation of the

accounting provisions of the Foreign Corrupt Practices Act (FCPA).

- Tampa - A shooting outside a nightclub in Ft. Myers left two teenagers dead and more than a dozen people wounded. Tampa referred media to Ft. Myers police, who are handling the investigation.



b7E

=====
Classification: UNCLASSIFIED//~~FOUO~~

[REDACTED]

From: [REDACTED]
Sent: Tuesday, July 26, 2016 5:06 PM
To: [REDACTED]
Subject: OPA Horizon - 7/26/2016 --- UNCLASSIFIED//~~FOUO~~

Classification: UNCLASSIFIED//~~FOUO~~

=====

Sent for Approval for RECORD//Sentinel Case 80-HQ-A1199962-HORIZON

**FBI Office of Public Affairs
The Horizon
 Tuesday, July 26, 2016**

National Issues

- PPD-41: OPA – Lisa Monaco at the International Conference on Cyber Security at Fordham University today announced the White House release of PPD-41, a Presidential Policy Directive aimed at coordinating a unified USG response to significant cyber incidents. OPA prepared the following statement to be issued upon request: “We at the FBI are excited about the announcement of PPD-41 and committed to the PPD’s interagency coordination structure to strengthen and streamline the USG response to significant cyber incidents. The FBI will play a key role as the lead for threat response. Protecting the United States from cyber attacks and intrusions by criminals, overseas adversaries, and terrorists is a top priority for the FBI. The threat of significant cyber incidents continues to grow, and we are very supportive of the creation of this strategy to help us protect the American public, businesses, organizations, and our national security.”
- Executive Announcements: OPA – OPA issued a press release to announce four new assistant directors. John Adams will be the new AD for the DI; David Resch will be the new AD for Training Division; Robert Jones will be the new AD for WMDD; and William Sweeney, Jr. will be the new ADIC of the New York Division.
- Comey message: OPA – ABC posted a web story this afternoon mentioning some of the comments the Director made in an internal message to employees. The story focused on mention of the Hillary Clinton investigation and did not include other topics brought up, or that it was part of a message celebrating the FBI’s 108th birthday. OPA is working on a response to place the video in the appropriate context.
- MH370: OPA – Multiple media inquiries over the last couple days about reports the FBI provided a report to the Government of Malaysia about the Malaysia Airlines flight that disappeared in 2014. OPA declined to comment and referred reporters to Malaysian authorities.
- DNC Emails: OPA – Continued to receive multiple media inquiries on the recent reporting of the Wikileaks release of DNC emails. OPA coordinated with the Cyber Division and released the following statement to media regulars: “The FBI is investigating a cyber intrusion involving the DNC and is working to determine the nature and scope of the matter. A compromise of this nature is something we take very seriously, and the FBI will continue to investigate and hold accountable those who pose a threat in cyberspace.” The statement was attributed to the FBI as an organization.

- Ransomware, DNC Emails: OPA - EnergyWire requested information and stats on ransomware, as well as the DNC hack statement. Provided updated stats and statement.

Local Stories

- Albuquerque - Sandia National Laboratories' newspaper interviewed Albuquerque Special Agent Bomb Technician [REDACTED] for an upcoming article. [REDACTED] discussed the XTK software developed by SNL for bomb technicians. The working partnership between the Department of Energy and bomb technician programs throughout the country was also highlighted.
- Boston - [REDACTED] was sentenced in U.S. District Court in Boston to six months in prison and two years supervised release for possession of a firearm with an obliterated serial number. The weapon had been transferred to another individual who then provided it to Dzhohkar Tsarnaev, one of the Boston Marathon Bombers. On April 18, 2013, the Ruger was used by the Tsarnaev brothers to kill MIT Police officer Sean Collier.
- Boston - The FBI Boston Division's SWAT Team arrested a convicted felon who was charged in connection with making threats over Facebook against Boston's largest mosque. [REDACTED] [REDACTED] was also charged with being a convicted felon in possession of ammunition. Following the arrest, the Evidence Response Team conducted a day-long search at his residence. The Division referred media outlets to the charging documents and press release issued by the US Attorney's office in Massachusetts.
- Chicago - FBI Chicago executed arrest warrants on 23 individuals charged with RICO violations and other charges. The operation targeted gang members in the city of Chicago. The arrests were made by FBI Chicago Agents, our local and federal partners, and neighboring FBI Division SWAT Teams. SAC Michael Anderson spoke at the U.S. Attorney's office press conference discussing today's arrests.
- Jacksonville - The U.S. Attorney's Office announced [REDACTED] and [REDACTED] were convicted of conspiracy, interfering with commerce by robbery, and using a firearm during a crime of violence in a multi-state jewelry store robberies case that was led by the Panama City RA. Co-conspirator [REDACTED] pleaded guilty on July 11. Between April 2015 and January 2016, the conspirators robbed six jewelry stores in Panama City Beach, Florida; Woodstock and Dawsonville, Georgia; Bluffton, South Carolina; Sevierville, Tennessee; and Mebane, North Carolina. More than \$4 million in jewelry was stolen during the time frame of the conspiracy.
- Louisville - [REDACTED] a former deputy with the Bullitt County, Ky., Sheriff's Office was found guilty by a federal jury following a four-day trial. Corder was convicted of two counts of willfully depriving a resident of his constitutional rights under the color of law.
- Newark - SA [REDACTED] spoke in Spanish to Univision regarding Newark fugitive [REDACTED] [REDACTED] FBI Newark is offering a \$20,000 reward for information leading to the arrest of [REDACTED] for his involvement in a MS-13 homicide. The segment will air Wednesday.
- New York - More than 15 reporters from national media outlets (Washington Post, CNN, ABC, etc.) attended the opening session of FBI-Fordham University's International Conference on Cyber Security. The session included remarks by NY ADIC Rodriguez and Cyber AD Trainor. White House Homeland Security Advisor Lisa Monaco announced a cyber presidential directive.
- San Juan - SAC Douglas A. Leff participated in a televised interview with [REDACTED] reporter for local ABC affiliate ABC5. SAC Leff also was the guest speaker at the monthly meeting of the Puerto Rico Hotel Security Association. Topics included FBI investigative priorities, terrorism, violent crimes, and public corruption. In both instances, SAC Leff urged the public to be aware of their surroundings and report any suspicious activity to the FBI and local authorities.

b6
b7Cb6
b7Cb6
b7C



=====
Classification: UNCLASSIFIED//~~FOUO~~