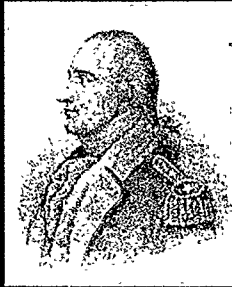


Bonus Question:

- Why did Benedict Arnold betray America?
 - Arnold was upset that he was not getting the credit he deserved for his actions during the Revolutionary War.



Insider Threat

- Anyone with legitimate access to information, technology, facilities, or personnel
 - Access is used to provide sensitive/classified information to an unauthorized person
- Or
- Access is used to degrade operations or capabilities

Who Are the Insiders?

- Over 4 million US clearance holders
- 860,000 have Top Secret Clearances
- 10,000 locations across the US
- How many people have access to proprietary or restricted information?

Categories of Threats

- Spills
 - Mishandling, careless, too much info on social networking sites
- Leaks
 - Wiki, media, bloggers, Twitter, media friends
- Espionage
 - Traditional spy
- Sabotage
 - Cyber, physical damage, damage to the reputation

It Doesn't Matter Where the Loss Occurs

- Classified information could be compromised at any location:
 - Military installation
 - US Government facilities
 - Cleared Defense Contractors
 - Research facility
 - College/University
- "WikiLeaks"

This Isn't Just a CI Problem

- Foreign governments, terrorist organizations, organized crime rings, drug cartels, etc., all want to know:
 - ✓ Who is the FBI investigating? *Cases*
 - What is the FBI doing? *Operations*
 - ✓ How does the FBI do it? *Methods*
 - What can the FBI do? *Capabilities/Limitations*
 - What does the FBI know? *Intelligence*
 - Who is helping the FBI? *Sources*

Insider Threats Require a Team Effort


- ⊙ Counterintelligence
- ⊙ Security
 - IT Security
- ⊙ HR
- ⊙ General Counsel
- ⊙ Risk Management (if applicable)

Why do people spy?

Why?


1. Divided Loyalty
2. Disgruntled
3. Ego
4. Financial Gain

FBI "Hall of Shame"




Richard Miller

- Special Agent - 1984
- Spied for Soviet Union from 1980 - 1984
- 20 years in prison
- *Financial Gain*

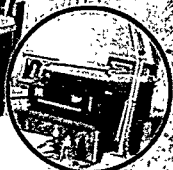


FBI "Hall of Shame"




Doug Tsou

- Language Analyst – 1988
- Spied for Taiwan
- 10 years in prison
- *Divided Loyalty*




FBI "Hall of Shame"




Earl Pitts

- Supervisory Special Agent – 1996
- Spied for Soviet Union/Russia from 1987 - 1992
- 27 years in prison
- *Disgruntled; Financial Gain*




FBI "Hall of Shame"




Robert Hanssen

- Supervisory Special Agent – 2001
- Spied for Soviet Union/Russia from 1979 - 2001
- Life in prison
- *Ego; Financial Gain; Disgruntled*




FBI "Hall of Shame"







Leandro Aragoncillo







- Intelligence Analyst – 2005
- Spied for the Philippines from 2000 - 2005
- 10 years in prison; \$40,000 fine
- *Divided Loyalty*



"So this is how it ends?"

"Hall of Shame" cont'd

John Connolly

Shamai Leibowitz – 2009
FBI Contract Linguist

James J. Smith – 2003
FBI Supervisory S...

b6
b7C

Espionage Indicators

Espionage Indicators

1. Disgruntled to the point of wanting retaliate against the government
2. Divided loyalty to a country besides the United States
3. Working odd hours without authorization
4. Removing classified materials without authorization
5. Seeking and/or obtaining classified information without a need-to-know

Espionage Indicators (cont'd)

- 6. Bringing unauthorized recording devices (thumb drives, cameras, cell phones) into work areas
- 7. Unnecessary photocopying of classified materials
- 8. Unexplained/Unreported foreign travel
- 9. Unreported foreign contacts
- 10. Unexplained affluence
- 11. Bragging about what they know

Espionage Indicators

- ⦿ These are common espionage indicators, not every spy exhibits all of these indicators
- ⦿ Not everyone who exhibits some of these indicators is a spy

Disgruntled...

...to the point of wanting retaliate against the government



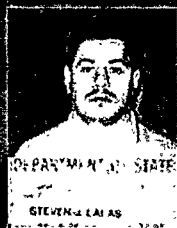
Divided Loyalty...

...to a country (or cause) besides the United States



Working Odd Hours...

... without authorization




Removing classified materials...

... without authorization




Seeking/Obtaining Classified Information...

...without a need-to-know




Unauthorized Recording Devices...

...brought into work areas, including: thumb drives, cameras, cell phones




Unnecessary Copying...

...of classified materials




Unexplained or Unreported Foreign Travel



Unreported Foreign Contacts

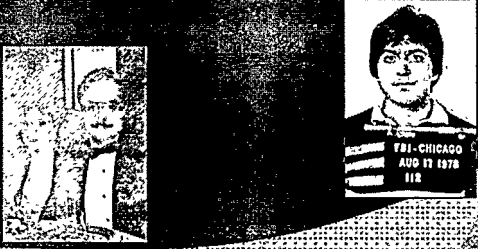


Unexplained Affluence



Bragging...


... about what they know



Is the Insider Threat more serious now?

Technology and Logistics

- o Because of technological advances, the logistics of stealing information have changed
 - 64 gigabyte USB drive holds a semi truckload of pages (approx. 4 million pages of MS Word docs)
 - No longer need to touch the information to steal/copy/photograph it
 - Imagine the risks of "cloud" networks



Why So Serious?

- o Why do Insiders pose such a great risk?
 - Access
 - Quality or quantity
 - o Robert Hanssen vs. WikiLeaks
 - They know what is most valuable
 - IT Security looks for hacks/intrusions from outside
 - Hide in plain sight

Exports

Quiz

1. (T/F) Since this information is NOT classified, I can share it with anyone.
2. (T/F) Because of where I work, I am a potential target for Espionage/Economic Espionage?
3. (T/F) He/she is here in the U.S., so it doesn't matter if we talk about unclassified information.
4. (T/F) Exports are always products shipped overseas.

The FBI Recognizes That:



- ⊙ Knowledge knows no boundaries
- ⊙ Global competition is beneficial
- ⊙ The flow of information is vital

Exports: Defined

- ⊙ Transfer of Anything to a "Foreign Person" or a foreign location by any means, anytime, anywhere, or a transfer to a "U.S. Person" when there is a knowledge that the items will be given to a "Foreign Person"

Provision of anything identified for protection by the U.S. Government to any foreign person, in any location.

Export Controls

- ⊙ Several types of export controls:
 - Export Administration Regulations (EAR) – Dept. of Commerce; "Dual-use"
 - International Traffic in Arms Regulations (ITAR) – Dept. of State; Defense articles, services, etc.
 - Arms Export Control Act
 - International Emergency Economic Powers Act (IEEPA) – Economic and trade sanctions

Fundamental Research: Defined

- ⊙ Basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.

• NSDD 189

Fundamental Research Exclusion

- ⊙ Does NOT apply if the language of the contract:
 - Forbids the participation of foreign persons;
 - Gives the sponsor or the other party to the agreement a right to approve publications resulting from the research; or
 - Otherwise operates to restrict participation in research and/or access to and disclosure of research results.
- ⊙ Both basic and applied research can be subject to export controls depending on the funding source and other delineated restrictions in place in a research contract.

Better to Be Safe

- ⊙ Contact _____ *before* sharing any information that may be restricted, including:
 - Security Office
 - Export Control Office
- Sharing includes: publications, emails, presentations, conversations, transfers, or any other exchanges of information
- ⊙ Export control is complex! Ask an expert.
 - Protect yourself
 - Protect your job
 - Protect your country

Penalties

- ⊙ Failure to comply with U.S. export control laws can result in severe penalties that can include the following:
 - Civil penalties up to \$500,000 for each violation;
 - Criminal penalties up to \$1,000,000 for each violation; and/or
 - Imprisonment for up to 10 years

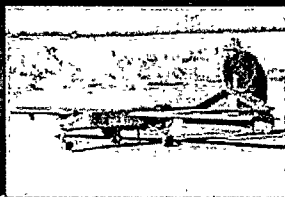
Dr. J. Reece Roth



- ⊙ Professor Emeritus of Electrical Engineering and Computer at the University of Tennessee, Knoxville
- ⊙ Specialist in plasma related research
- ⊙ Multiple patents, many leased to Atmospheric Glow Technologies
- ⊙ Now retired

The Charge

- ⊙ "Between January 2004 and May 2006, Roth and AGT engaged in a conspiracy to transmit export-controlled technical data related to a restricted U.S. Air Force contract to develop plasma actuators for a munitions-type UAV, or "drone," to one or more foreign nationals, including a citizen from the People's Republic of China."



Targeting Techniques

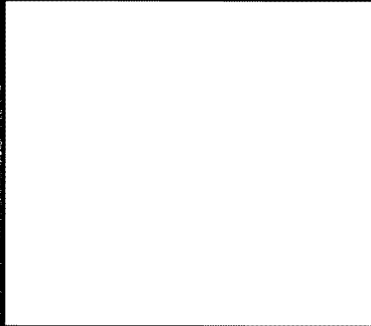
"Bummer of a birthmark, Hal."



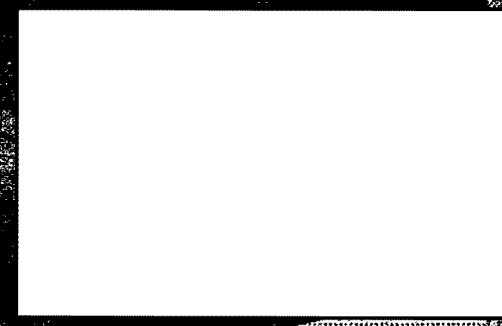
Information = \$

- ⊙ "Because that's where the money is." – Willie Sutton on why he robbed banks.
 - Information is the new currency
 - You are the new "banks"
- ⊙ Be thankful you are a target
 - An organization with no information or ideas to protect has no reason to exist
 - Our information/ideas are what separate us from our competitors
 - And it gives YOU a job!

Targeting Techniques




Vulnerabilities




b7E

How Are They Successful?




- ◉ "We have ways of making you talk."
 - Col. Klink from *Hogan's Heroes*

How Are They Successful?



b7E


Social Media



- ◉ NEVER post anything sensitive or classified (or even hints at sensitive/classified information)
 - Avoid posting anything work-related

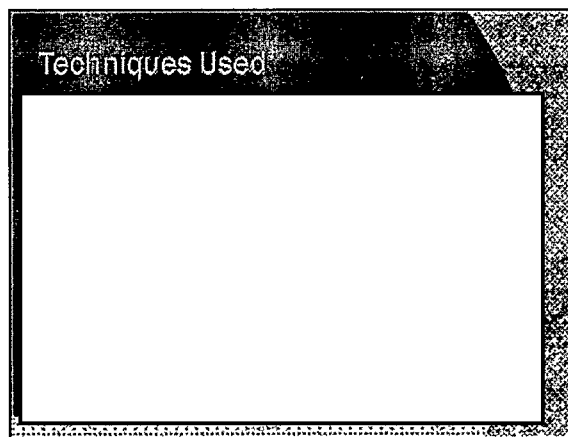
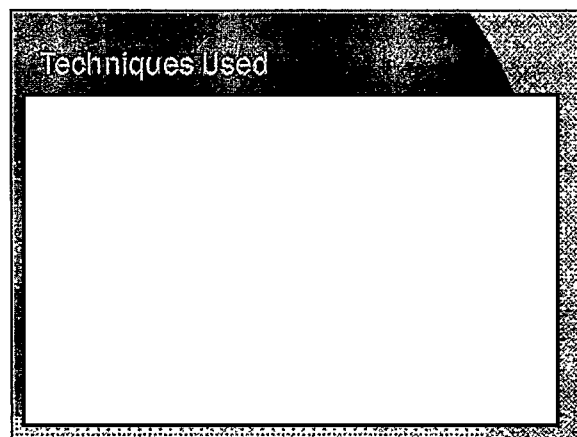
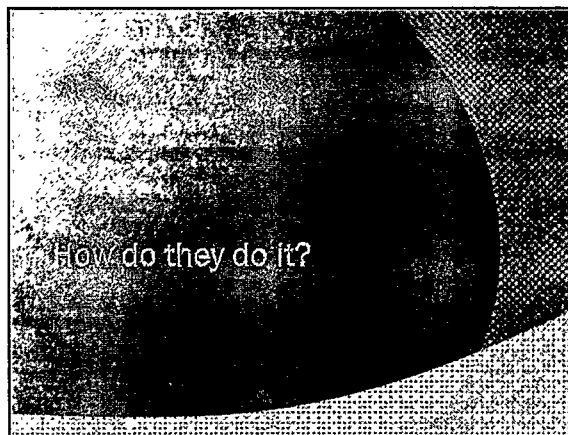
Robin Sage

- ◉ Cyber Threat Analyst
 - 25 years old
 - MIT graduate
 - 10 years work experience
- ◉ Naval Network Warfare Command, Norfolk, VA
- ◉ In 19 days (12/2009 – 01/2010)
 - Over 300 contacts on Facebook, LinkedIn, Twitter
 - ◉ Mostly military, intelligence, security personnel, including: Government, military, cleared defense contractors
 - Job offers
 - Offers for speaking engagements
- ◉ 100% fictional

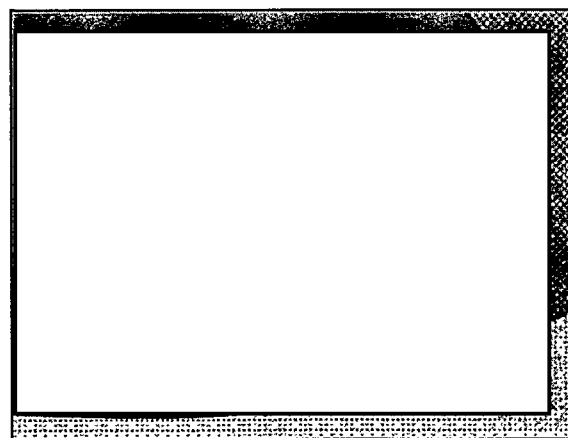
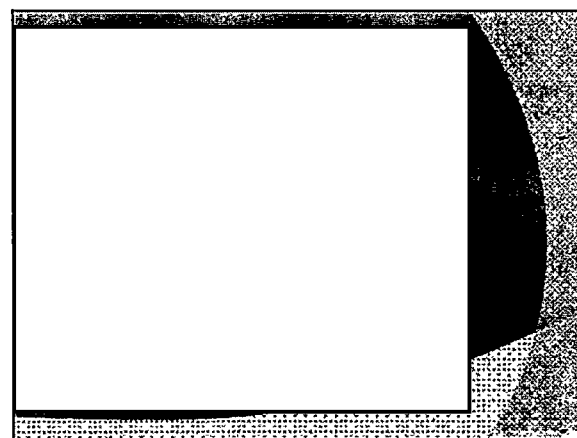


"Robin Sage" picture used on social media sites. (Picture not to scale)

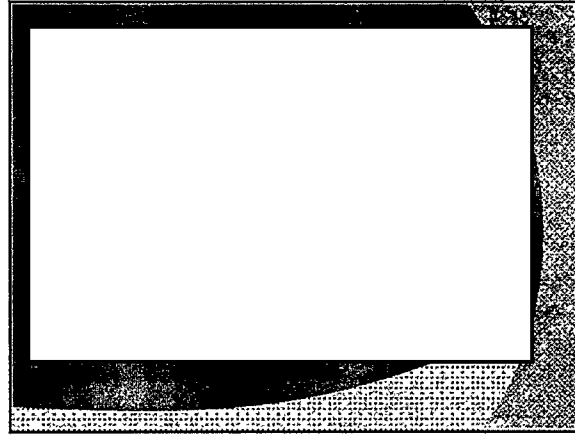
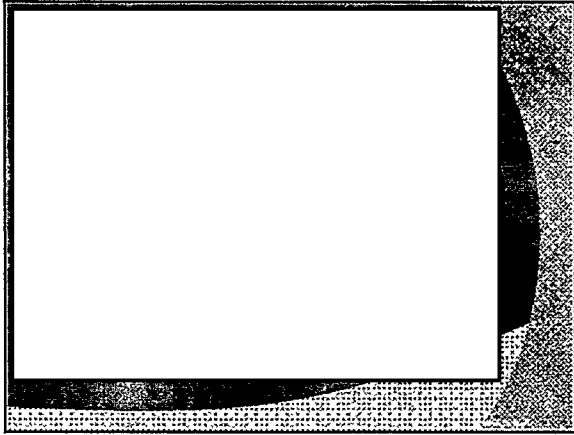
b7E



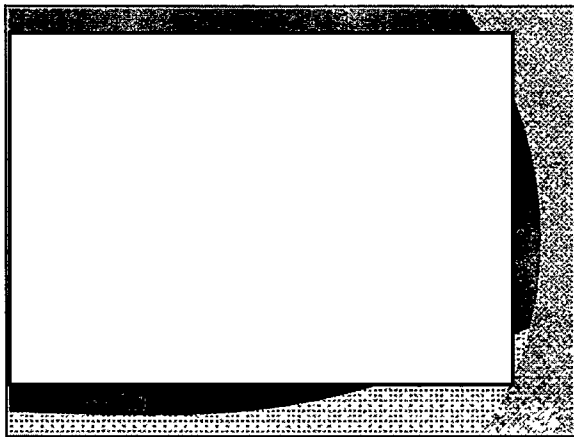
b7E



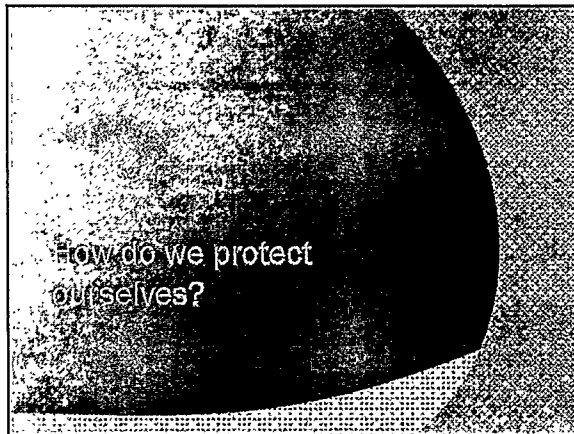
b7E



b7E



b7E



Insanity

- ◉ "Doing the same thing over and over again and expecting different results."
 - Albert Einstein
- ◉ Application to business:
 - Thinking our adversaries/competitors will steal from everyone else, but not from us.

When Traveling

- ⊙ Don't take anything you don't need
 - Information – including personal information
 - Electronic devices – "Smart phone" + foreign travel = dumb/idea
 - Extra credit cards
- ⊙ Assume that *everything* you take with you will be searched
 - All information on computers, phones, electronic media, and in documents will be taken/copied
 - Do not leave your things unattended: bags, electronic devices, drinks
- ⊙ Obey local laws/customs
 - Don't get caught in a compromising position
- ⊙ Be wary of people you meet
 - International date line
- ⊙ You have no expectation of privacy while there

Need to Know

- ⊙ Each of us practice "need to know" everyday in our private lives
 - Bank account numbers
 - Social security numbers
- ⊙ Make sure someone has a need to know about your research before you share *any* information with them
 - Don't just take *their* word for it

What are they after?

Why R&D?

- ⊙ Research and Development (R&D)
 - Expensive
 - Time & labor intensive
 - "Cutting edge"
 - Biggest potential payoff – new technologies, markets
- ⊙ Anywhere we have an advantage
 - Not just military technology
 - Could be anything from growing food to weather simulation to advanced weapons
- ⊙ Failures & dead ends
- ⊙ All of the easy problems were solved long ago
 - That leaves the difficult problems
 - More difficult = more expensive

Examples

⊙ Employee data	⊙ Classified projects
⊙ Phone directories	⊙ Proprietary formulas and processes
⊙ Computer network design	⊙ Technical components and plans
⊙ Computer access protocols	⊙ Research grant applications
⊙ Passwords	⊙ Sensitive but unclassified research

What to report?

When to Report?

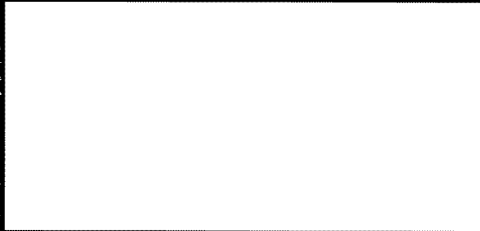
- ⊙ If you wonder whether you should report something, report it
- ⊙ As soon as you think there might be a problem
- ⊙ The sooner a problem is identified, the sooner it can be dealt with
- ⊙ Bad news does not improve with age

If You See Something, Say Something

- ⊙ Follow _____'s established procedures to report
 - Foreign travel
 - Foreign contacts
 - Suspicious behavior

Report Suspicious/Unusual Activity

- ⊙ You should report any suspicious activity/occurrences



Report Suspicious/Unusual Activity

- ⊙ You should report any suspicious activity/occurrences



- ⊙ If you wonder, "should I report this?" – then YES you should!

b7E

Questions?

SSA _____
 Insider Threat Program Manager

Insider Threat Investigations Unit (CD-4D)
 Counterespionage Section
 Counterintelligence Division



b6
b7C

OPM's Strategic and Operational Plan

- In the interests of our national security...all employees shall be:
 - Reliable
 - Trustworthy
 - Of good conduct and character
 - Of complete and unswerving loyalty to the United States

Adjudicative Guidelines

- For Determining Eligibility for Access to Classified Information (12/29/2005)
 - Allegiance to the U.S.
 - Foreign Influence/Preference
 - Sexual Behavior
 - Personal Conduct
 - Financial Considerations
 - Alcohol Consumption/Drug Involvement
 - Psychological Conditions
 - Criminal Conduct
 - Handling Protected Information
 - Outside Activities
 - Use of Information Technology Systems

Allegiance to the U.S.

Montes - DIA
Squillacote - DoD
JULIUS ROSENBERG
XITELL ROSENZWEIG

Foreign Influence/Preference

Montaperto - DIA
Aragoncillo - FBI
TGOU - FBI


Sexual Behavior

Miller - FBI
Jean-Pierre
Smith - FBI

Financial Considerations

Ames - CIA
Aragoncillo - FBI
Pollard - Navy
Pellon - NSA
Walker - Navy

Alcohol Consumption (Abuse/Alcoholism)




LANCE ALMON ELSTER
DOB 04-28-41
PIC 644-MF-004423
FM 8870 2-21-84

Drug Involvement


- Roderick Ramsey (part of the Clyde Conrad spy ring) recruited at least two other soldiers to participate in espionage:

"The people that I recruited, yes, they were involved in drugs, but it wasn't so much that they were pot smokers or hashish smokers that made them, in my opinion, more susceptible to the pitch. It was that these were people who had already shown a propensity or willingness to violate Army regulations."

Anyone in the Army who was willing to take drugs on a regular basis has to be willing to take some kind of risk and has to be willing to break the Army's regulations. That's the starting point."




Ramsey - Army




Personal Conduct


- Patterns of dishonest, unreliable, or rule-breaking behavior.




Ramsey - Army




DAVID S. BOONE
DOB 04-28-41
PIC 644-MF-004423
FM 8870 2-21-84




LANCE ALMON ELSTER
DOB 04-28-41
PIC 644-MF-004423
FM 8870 2-21-84




Psychological Conditions




Pollard - Navy




Hanssen - FBI




Boyce - Contractor



LANCE ALMON ELSTER
DOB 04-28-41
PIC 644-MF-004423
FM 8870 2-21-84




Criminal Conduct




Connolly - FBI

Handling Protected Information




Aragocillo - FBI



Pollard - Navy

b7E

Use of Information Technology Systems



Outside Activities

- Often related to foreign contacts, or activities that conflict with organization's security/policies:
 - Samuel Morrison – Office of Naval Intelligence provided classified information to *Jane's*

Background Investigators

Why Are You a Target?

- Fact [redacted]
- Why? [redacted]

b7E

One More Thing..

[redacted]

Job Offers

- Often will approach targets with lucrative job offers overseas
 - Consulting
 - Private Investigations
 - Security related

b7E

OPM's Strategic and Operational Plan


- ⊙ In the interests of our national security ...all employees shall be:
 - Reliable
 - Trustworthy
 - Of good conduct and character
 - Of complete and unwavering loyalty to the United States

Your Mission:

Should you choose to accept it:


- ⊙ You will perform checks on more people
- ⊙ You will have less time
- ⊙ You will be limited in the questions you can ask

Efficiency vs. Threat



We need you...

YOU are the 1st Line of Defense



b7E

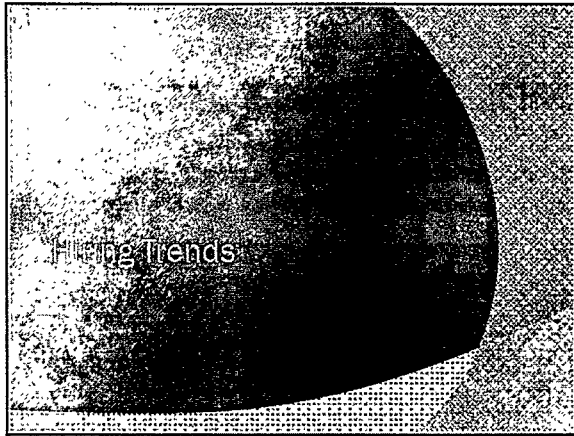
Factors of Concern

- ⊙ Extent of classified access
- ⊙ Intelligence officer/foreign government official contact
- ⊙ Foreign contacts and travel particularly if unreported
- ⊙ Furtive removal of classified material

What you can do....

- ⊙ Get names in original language
- ⊙ Finances (Determine if there are any issues)
 - It is difficult to live/work overseas for years without a foreign bank account
- ⊙ Ask for details on foreign organizations, including:
 - Name of organization in English and original language
 - Purpose of the organization
 - Membership in the organization
 - Foreign intelligence services often use organizations as cover, or for spotting/assessing
- ⊙ Follow up on foreign contacts (contact info)
 - Includes: email contacts, social networking contacts, etc.
- ⊙ Contact with foreign intelligence/police/security
 - FIS often use police

If you suspect something, Flag it for follow up



What are we currently seeing?

- ◉ More applicants from foreign countries applying for IA or SA positions
 - Applicants lived/worked overseas
- ◉ Dates in applications not matching
- ◉ Applicants marrying to gain citizenship
- ◉ Close family members living in a foreign country
- ◉ Unreported foreign contacts
- ◉ Lack of verifiable information

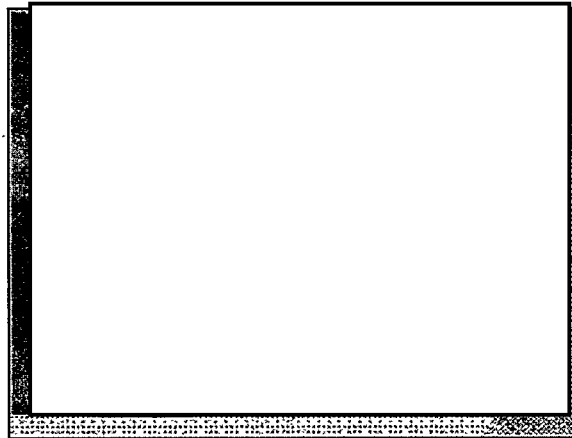


b7E

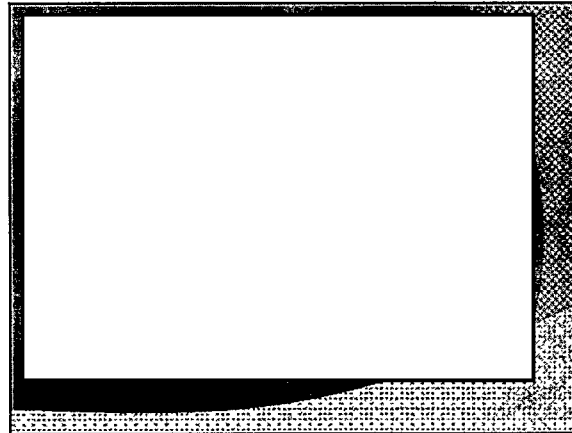
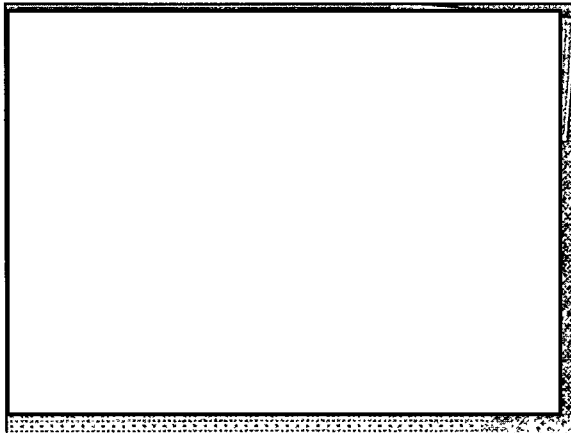
Glenn Shriver



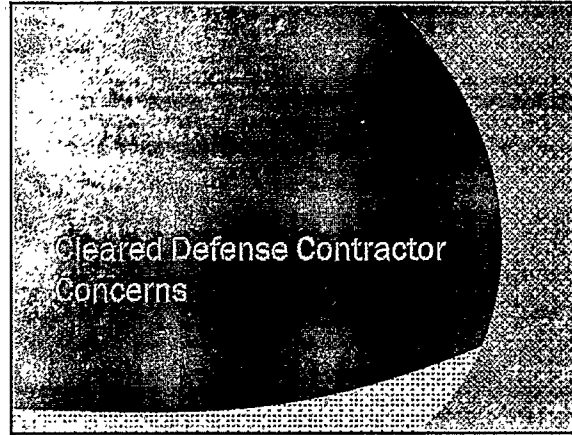
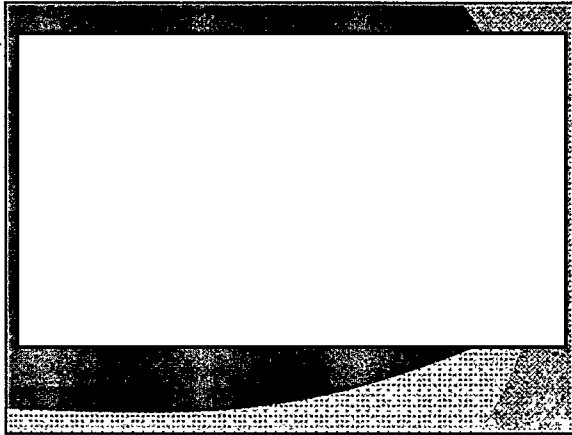
- ◉ Studied in Shanghai – 2002-2003
- ◉ Moved to PRC – responded to ad
- ◉ Contacted by Chinese IOs
- ◉ Took DoS FSO exam twice/applied to CIA
- ◉ Guilty plea 10/2010 (Conspiracy to transmit NDI)
- ◉ 4 year sentence
- ◉ PRCEMB spokesman – The PRC states it “never engages itself in activities that’ll harm other countries’ national interests, and it is sincere in developing Sino-U.S. relations of mutual benefit.”



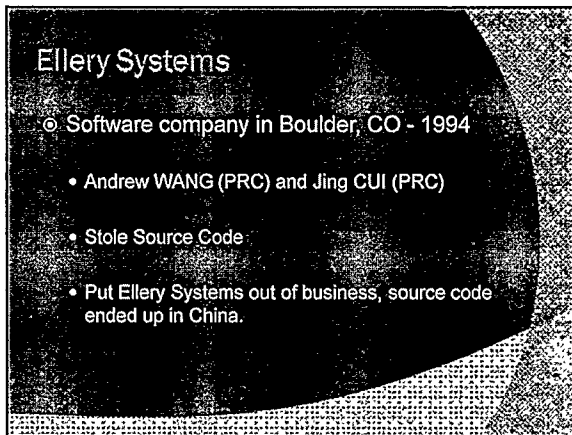
b6
b7C



b6
b7C
b7E

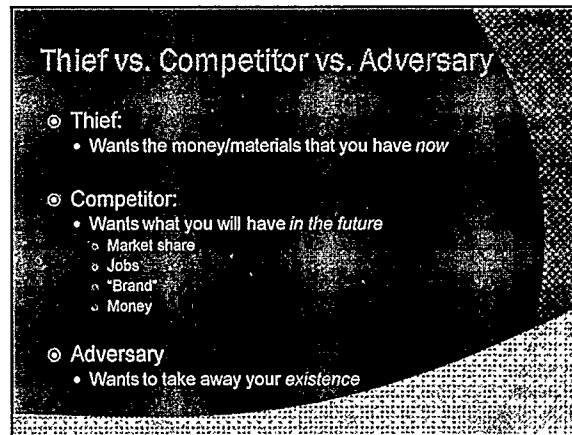


b6
b7C
b7E



Ellery Systems

- Software company in Boulder, CO - 1994
 - Andrew WANG (PRC) and Jing CUI (PRC)
 - Stole Source Code
 - Put Ellery Systems out of business, source code ended up in China.



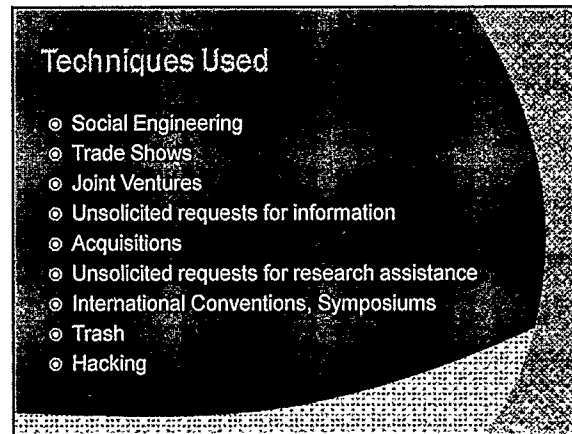
Thief vs. Competitor vs. Adversary

- Thief:
 - Wants the money/materials that you have *now*
- Competitor:
 - Wants what you will have *in the future*
 - Market share
 - Jobs
 - "Brand"
 - Money
- Adversary
 - Wants to take away your *existence*



In the News

- Examples of Economic Espionage/Theft of Trade Secrets:
 - Wen Chyu "David" Liu - Dow Chemical
 - Michael Mitchell - DuPont
 - Meng Hong - DuPont
 - Shalin Jhaveri - Bristol-Myers Squibb
 - Hanjuan Jin - Motorola
 - Sergey Aleynikov - Goldman Sachs
 - David Lee - Valispar
 - Dongfan "Greg" Chung - Boeing



Techniques Used

- Social Engineering
- Trade Shows
- Joint Ventures
- Unsolicited requests for information
- Acquisitions
- Unsolicited requests for research assistance
- International Conventions, Symposiums
- Trash
- Hacking

Cost of Doing Business

- Many companies view Economic Espionage as "the cost of doing business"
 - The cost continues to rise. Some estimates are equal to U.S. companies **spend more than \$1 Trillion per year**
 - Eventually, the cost will be too great to bear
 - Then it will be too late!

Take Responsibility

- Know what is most important to your organization
 - The more important information is, the fewer the number of people that should have access to it.
 - What are your company's strengths?
 - This is what your competitors will be after.

Really Bad Signs

- Those who fail to learn from history are doomed to repeat it.
 - William Faulkner

Mitigation Strategies for Organizations

b7E

Mitigating the Threat

- Education and training of workforce
- Computer banners and Non-disclosure agreements
 - You should have policies in place which allow you to monitor computer activity of employees
 - Cannot rely solely on these to protect you
 - You get what you *inspect*, not what you *expect*
- System must utilize *active alerts*

Mitigating the Threat

- High risk business activities:
 - Foreign Operations
 - Joint Ventures with Foreign Partners
 - Foreign Travel
 - Trade Shows
- Don't take what you don't want "them" to get

Mitigating the Threat: Travel

- o Foreign travel – a high risk activity
 - Require employees to notify company of personal foreign travel
 - Provide threat briefings
 - Ask tough questions:
 - o Will you be meeting anyone related to your work?
 - o Will you be conducting any speaking engagements – formal or informal?
 - o Will you be taking any information/materials from work?


Mitigating the Threat: Travel

- o Foreign travel – a high risk activity (cont'd)
 - "Smart phone" + foreign travel = dumb idea
 - Prevent remote logging into computer network
 - o Even a "secure" connection will be using foreign internet connection
 - Require any company laptops, phones, etc. to be turned in while on travel
 - Buy "stripped down" laptop/phones for employees to use when on foreign business travel
 - o Destroy hard drive after trip
 - o Never connect to your network with these devices

When Traveling

- o Don't take anything you don't need
 - Information – including personal information
 - Electronic devices
 - Extra credit cards
- o Assume that *everything* you take with you will be searched
 - All information on computers, phones, electronic media, and in documents will be taken/copied
 - Do not leave your things unattended: bags, electronic devices, drinks
- o Obey local laws/customs
 - Don't get caught in a compromising position
- o Be wary of people you meet
- o You have no expectation of privacy while there

Place to go



b7E

Mitigating the Threat

- o When entering joint venture/partnership:
 - Consider creating a completely independent computer network with NO connectivity to main network
 - Realize the potential risks as well as the potential gains

Mitigating the Threat

- o Identify "high risk" users:
 - Significant foreign influence
 - Financial hardship
 - Underperforming (and advised as such)
 - Facing administrative/disciplinary action
 - Facing potential layoff or job termination

Mitigating the Threat

- Identify "high risk" behavior:


- User context
 - Different users have different accesses

811 Referrals

b7E

Section 811


- Intelligence Authorization Act of 1995
- Head of each agency in the Executive Branch shall ensure the FBI is advised immediately of any information indicating classified information has/is being disclosed to a foreign government without authorization



Section 811

Responsibilities of other agencies

- Ensure FBI is consulted regarding all subsequent actions to determine the source of the loss
- Given complete and timely access to agency employees and records
- Avoid alerting subjects to the FBI investigation



Section 811

Responsibilities of the FBI

- FBI will ensure that information developed as a result of the investigation relating to:
 - Espionage information relating to their personnel
 - Information on operations and risks

FBI will consult with the referring agency regarding the espionage investigation

Section 811

- Waiver
- In extraordinary circumstances affecting vital national security interests, the President may waive the preceding requirements as they apply to the head of a particular department of agency

Section 811

- 811 does not apply to:
 - Media Leaks
 - Security Violations



COMSEC

Why is COMSEC important?

- A historical example of exploiting an enemy's communications
- The setting:
 - May, 1942 in the Pacific
 - Japanese advance since Pearl Harbor:
 - Philippines
 - Malaya
 - Singapore
 - Dutch East Indies (Indonesia)
 - Thailand
 - Hong Kong
 - Guam
 - Wake Island

COMINT in Action

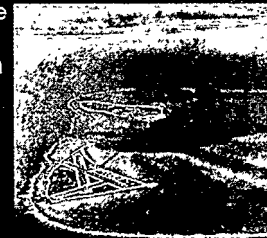
- The U.S. broke Japan's JN25 code and were able to prevent Japan's capture of Port Moresby, New Guinea (Battle of Coral Sea) in early May, 1942.
- U.S. discovered Japanese were planning another attack on the U.S. at "AF" at the beginning of June, 1942.
 - Japan's plan was to set a trap for the U.S. to lure the aircraft carriers into reach
 - If successful, Japan would have total domination of the Pacific

The Plan

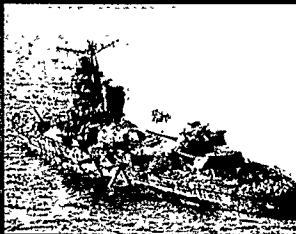
- To determine where "AF" was, the U.S. sent innocuous messages from various locations to determine "AF" in the clear
- Each possible location would send a message with a unique problem at the location. If the Japanese referred to any of the problems as being at "AF", it identifies their target

Where is "AF"? Midway

- Midway Island sent fake message that it had a broken water distillation plant, and the island needed fresh water
- Japanese sent coded messages that "AF" needs fresh water



The Result



- U.S. knew Japan's plan and set up an ambush
- U.S. scored a decisive victory
- Battle of Midway is called "the turning point of the war in the Pacific"

Communications-related Spies: 1975 - present



- Walker - Navy
- Whitworth - Navy
- Pelton - NSA
- Boone - Army/NSA
- Ramsay - Army
- Boyce - Contractor
- Lee - Civilian
- Lipka - NSA

Communications Spies (cont'd)

- Michael Allen - Navy
- Charles Anzalone - USMC
- Stephen Baba - Navy
- Jeffrey Carney - Air Force/NSA
- James Hall III - Army
- Joseph Helmich - Army
- Eric Jenott - Army
- Bruce Kearn - Navy
- Francisco Mira - Air Force
- Frank Nesbitt - USMC/Air Force
- Charles Slatten - Army
- Henry Spade - Navy
- Michael Tobias and Francis Pizzo - Navy

Worked at NSA

- David Boone - Army/NSA
- Jeffrey Carney - Air Force/NSA
- Robert Lipka - NSA
- Ronald Pelton - NSA

Had Access to a Code Room

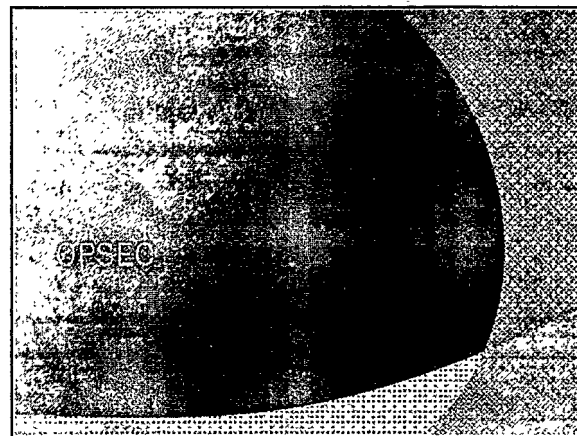
- Michael Allen - Navy
- Stephen Baba - Navy
- Christopher Boyce - Contractor
- Joseph Helmich - Army
- Eric Jenott - Army
- Steven Lalas - Dept. of State
- Robert Lipka - NSA
- Frank Nesbitt - USMC/Air Force
- Charles Slatten - Army
- Henry Spade - Navy
- Michael Tobias - Navy
- John Walker - Navy
- Jerry Whitworth - Navy

Gave Communication Plans/Techniques

- Charles Anzalone - USMC
- Christopher Boyce - Contractor
- Jeffrey Carney - Air Force/NSA
- James Hall III - Army
- Andrew Lee - Civilian
- Robert Lipka - NSA
- Francisco Mira - Air Force
- Frank Nesbitt - USMC/Air Force
- Ronald Pelton - NSA
- Roderick Ramsay - Army
- John Walker - Navy
- Jerry Whitworth - Navy

Gave Crypto

- ⊙ Charles Anzalone – USMC (Equip. manuals)
- ⊙ Stephen Baba - Navy
- ⊙ Christopher Boyce – Contractor
- ⊙ Joseph Helmich – Army
- ⊙ Bruce Kearns – Navy (publications)
- ⊙ Andrew Lee – Civilian
- ⊙ Francisco Mira – Air Force (code books)
- ⊙ Charles Slatten – Army
- ⊙ Henry Spade – Navy
- ⊙ Michael Tobias and Francis Pizzo- Navy
- ⊙ John Walker – Navy
- ⊙ Jerry Whitworth - Navy



How Did...

- ⊙ Poor OPSEC on 02/28/1993 lead to:

Waco, Texas 04/19/1996

And

Oklahoma City, Oklahoma 04/19/1995

OPSEC

“I’ve been thinking about your job and what you’re trying to do. Anything I can do to help, just let me know.”

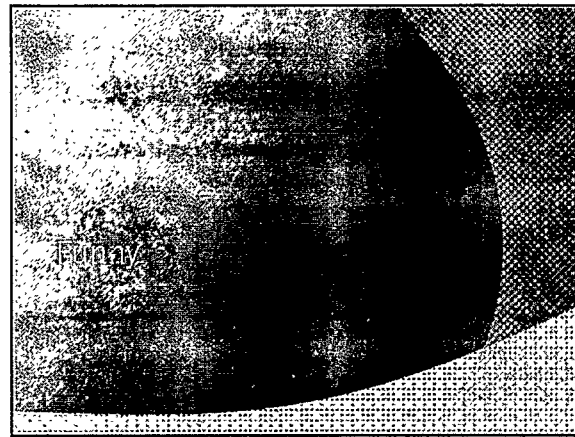
Russian spy Aldrich Ames to Chief of the CIA Mole Team

Need to Know

- ⊙ Each of us practice “need to know” everyday in our private lives
 - Bank account numbers
 - Social security numbers
- ⊙ Make sure someone has a need to know before you share *any* information with them
 - Don’t just take *their* word for it

Simple OPSEC Measures

- ⦿ Social Media – if you use it, never make any mention of work
- ⦿ Don't share information on where you work or what you do with strangers
- ⦿ Protect your passwords and building access codes like they are your ATM PIN



"They rubbed my tummy, chief – I told them everything."

O'Brien
"They rubbed my tummy, chief—I told them everything."

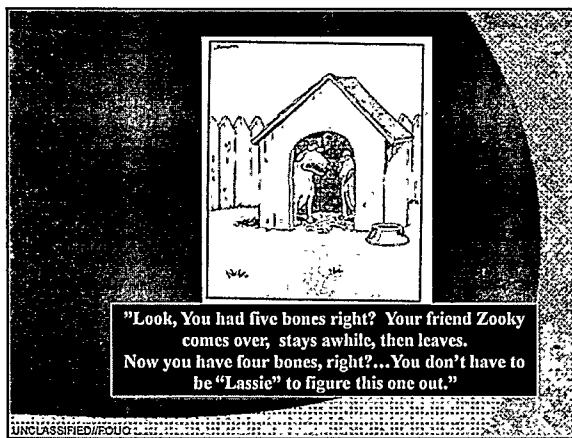
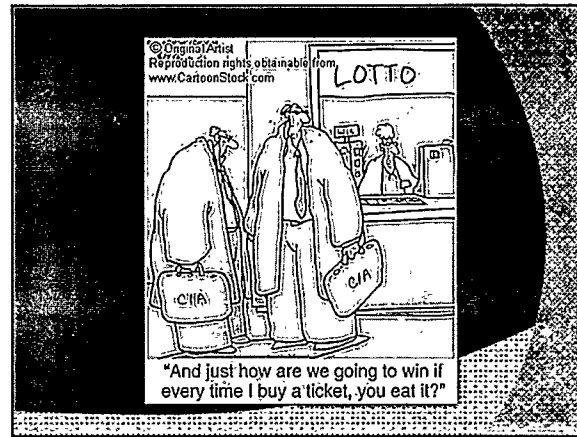
"The traitor moves within the gates freely, his sly whispers rustling through the alleys, heard in the halls of government itself. For the traitor speaks in accents familiar to his victims and he wears their face and their garments."
Roman statesman Marcus Tullius

off the mark by Mark Parisi
www.offthemark.com

Houston, it's very possible we're being tracked by spy satellites...

It's a Jungle out there by HAGEN

The peck became suspicious! The newcomer was asking too many questions about tomorrow's hunt



UNCLASSIFIED//FOUO

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1261025-0

Total Deleted Page(s) = 36

- Page 4 ~ b5; b7E;
- Page 5 ~ b5; b6; b7C; b7E;
- Page 6 ~ b5; b6; b7C; b7E;
- Page 7 ~ b5; b7E;
- Page 8 ~ b5; b6; b7C; b7E;
- Page 9 ~ b5; b7E;
- Page 10 ~ b5; b6; b7C; b7E;
- Page 11 ~ b5; b7E;
- Page 12 ~ b5; b6; b7C; b7E;
- Page 13 ~ b5; b6; b7C; b7D; b7E;
- Page 14 ~ b5; b6; b7A; b7C; b7D; b7E;
- Page 15 ~ b5; b6; b7A; b7C; b7D; b7E;
- Page 16 ~ b5; b6; b7A; b7C; b7D; b7E;
- Page 17 ~ b5; b7E;
- Page 18 ~ b5; b6; b7C; b7E;
- Page 19 ~ b5; b7E;
- Page 20 ~ b5; b6; b7C; b7E;
- Page 21 ~ b5; b7E;
- Page 22 ~ b5; b6; b7A; b7C; b7D; b7E;
- Page 23 ~ b5; b6; b7A; b7C; b7D; b7E;
- Page 46 ~ b5;
- Page 50 ~ b5; b6; b7C;
- Page 106 ~ Referral/Consult;
- Page 107 ~ Referral/Consult;
- Page 108 ~ Referral/Consult;
- Page 109 ~ Referral/Consult;
- Page 117 ~ Referral/Consult;
- Page 118 ~ Referral/Consult;
- Page 187 ~ b5;
- Page 191 ~ b5; b6; b7C;
- Page 204 ~ Referral/Direct;
- Page 205 ~ Referral/Direct;
- Page 418 ~ Referral/Consult;
- Page 419 ~ Referral/Consult;
- Page 443 ~ Duplicate;
- Page 444 ~ Duplicate;

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```


SENATE COMMITTEE ON THE JUDICIARY
OFFICE OF THE CLERK
433 SENATE CHAMBERS
WASHINGTON, D.C. 20540
TELEPHONE: 202-224-2000
FACSIMILE: 202-224-2000
WWW.SENATE.GOV

United States Senate

COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20540 6275

December 17, 2013

VIA ELECTRONIC TRANSMISSION

The Honorable James B. Comey, Jr.
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, DC 20535

Dear Director Comey:

On October 28, 2013, I received a letter from the Federal Bureau of Investigation (FBI) in which it indicated that it had collaborated with the Office of the Director of National Intelligence (ODNI) on two training videos about the FBI's National Insider Threat Program. The videos, titled *Betrayed* and *Game of Pawns*, were developed jointly by the FBI's Counterintelligence Division and ODNI's Office of the National Counterintelligence Executive (ONCIX). The FBI has also produced other insider threat materials, such as the brochure, *The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy*.¹

As I understand it, the National Insider Threat Program is the result of Executive Order 13587, issued by President Obama in October 2011, which established an interagency Insider Threat Task Force, to be staffed by the FBI and the ONCIX.² It also directed Executive Branch departments and agencies to develop their own insider threat programs. The President subsequently issued a Presidential Memorandum in November 2012 transmitting the National Insider Threat Policy and setting forth minimum standards for departmental and agency programs.³

These efforts have subsequently received press attention, some of which has focused on concerns about whether the program adequately protects whistleblowers.⁴

¹ Federal Bureau of Investigation, *The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy*, http://www.fbi.gov/about-us/investigate/counterintelligence/insider_threat_brochure.

² Executive Order 13587 – Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011. Available at <http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-structural-reforms-improve-security-classified-networks->.

³ Presidential Memorandum – National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Nov. 21, 2012. Available at <http://www.whitehouse.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand>.

⁴ For example, Marisa Taylor and Jonathan S. Landay, "Obama's crackdown views leaks as aiding enemies of U.S.," *McClatchy* (Jun. 20, 2013), available at

As you know, I strongly believe that whistleblowers play an important role in safeguarding the federal government against waste, fraud, and abuse. You too stated in your confirmation hearing that you believe whistleblowers are a critical element of a functioning democracy. Their willingness to come forward contributes to improving government operations. They often put themselves at risk of reprisal from their employers, sometimes being demoted, reassigned, or fired as a result of their actions. Under the Whistleblower Protection Act and Presidential Policy Directive 19, federal employees may not be retaliated against for reporting waste, fraud, and abuse.⁵

Accordingly, some agencies have taken steps to prevent the insider threat program from chilling whistleblower communications. For example, the Office of the Inspector General for the Intelligence Community is developing training that integrates whistleblowing into the agency processes, making the Intelligence Community whistleblowing and insider threat programs mutually reinforcing.

In order to assess whether training materials on the National Insider Threat Program provide adequate guidance on protecting whistleblowers, I respectfully request that you provide me with copies of *Betrayed* and *Game of Pawns*, as well as copies of any other training materials regarding the National Insider Threat Program or any FBI-specific insider threat program. I would appreciate receiving these materials by January 14, 2014. I know that you consider transparency to be an important value, and I trust that transparency on this issue will benefit both whistleblowers and our national security.

Should you have any questions regarding this letter, please contact [redacted]
[redacted] of my staff at [redacted]

b6
b7c

Sincerely,



Charles E. Grassley
Ranking Member

cc: The Honorable James R. Clapper
Director of National Intelligence

~~SECRET//NOFORN~~

FY 2012 Request to Congress Overview

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



March 24, 2011

~~SECRET//NOFORN~~



SECRET//NOFORN
Foreign Intelligence

(S)

FY 2012 Request [redacted] positions

b1
b3



(S)

[redacted]

[redacted]

[redacted]

[redacted]

b1
b3
b7E

(S)

Insider Threat

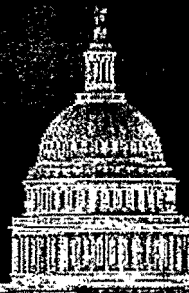
• Insider Threat remains the greatest vulnerability to the USG.

[redacted] to will acquire hardware, software and related contractor support for initial audit generation, collection, and monitoring capabilities.

• This initiative would provide useful analysis on insider threats and can provide early warning signs that can prevent the development of such threats. In addition the resources would allow the FBI to share information with the IC.



Office of CONGRESSIONAL Affairs



calendar

Week of August 1 - 5, 2011

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 03-03-2016 BY F22M45K38 NSICG

Updated: August 5, 2011 (7:00 a.m.)

Date	Time	Event	Topic	FBI Participants	Other Participants	Contact
Monday, August 1	9:30 a.m.	Senate Select Committee on Intelligence Staff Briefing [redacted]	Insider Threat Study	[redacted] Security; SC Randy Coleman-CD; [redacted]	N/A	[redacted]
Monday, August 1	11:30 a.m.	Staff Briefing-Senate Homeland Security and Governmental Affairs Committee	Community Outreach Efforts/Countering Violent Extremism (CVE)	UC [redacted]	DOJ/OLA: [redacted] DOJ: OLI [redacted] [redacted] Civil Rights [redacted] [redacted]; CRS [redacted] EOUSA/S [redacted] DOJ/OLA: [redacted]	[redacted]
Tuesday, August 2	9:30 a.m.	Senate Select Committee on Intelligence Staff Briefing - [redacted]	Insider Threat Investigations & prevention coordinated by CD	SC Randy Coleman & others	N/A	[redacted]
					DOJ/OLA [redacted]	

b6
b7c



U.S. Department of Justice
Federal Bureau of Investigation

Washington, D.C. 20535-0001

December 31, 2013


Honorable Charles E. Grassley
Ranking Member
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Senator Grassley:

This responds to your letter to Director Comey dated December 17, 2013, in which you requested copies of two training videos about the FBI's Insider Threat Program. The videos, titled Betrayed and Game of Pawns, were developed jointly by the FBI's Counterintelligence Division and the Office of the National Counterintelligence Executive (ONCIX). The videos are enclosed and are considered law enforcement sensitive for official use only, so we would request that you not disclose the videos further without contacting us.

If I can be of additional assistance in this or any other matter, please feel free to contact me at

Sincerely,


Stephen D. Kelly
Assistant Director
Office of Congressional Affairs

Enclosures

- 1 - Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510
- 1 - Honorable James R. Clapper
Director of National Intelligence

b6
b7c

December 31, 2013

Honorable Charles E. Grassley
Ranking Member
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Senator Grassley:

This responds to your letter to Director Comey dated December 17, 2013, in which you requested copies of two training videos about the FBI's Insider Threat Program. The videos, titled Betrayed and Game of Pawns, were developed jointly by the FBI's Counterintelligence Division and the Office of the National Counterintelligence Executive (ONCIX). The videos are enclosed and are considered law enforcement sensitive for official use only, so we would request that you not disclose the videos further without contacting us.

If I can be of additional assistance in this or any other matter, please feel free to contact me at

b6
b7C

Sincerely,

Stephen D. Kelly
Assistant Director
Office of Congressional Affairs

Dep. Director _____
 EAD-Adm. _____
 EAD-CTCI _____
 EAD-Imm. _____
 EAD-Intell. _____
 EAD-LES _____
 Asst. Dir.: _____
 Adm. Serv. _____
 CIS _____
 Crim. Inv. _____
 Crim. Inv. _____
 Cyber _____
 Finance _____
 Info. Res. _____
 Inspection _____
 Inv. Tech. _____
 Laboratory _____
 Off. of Cong. & Public Affs. _____
 Off. of the Sec'y _____
 Comm. _____
 Off. of Intell. _____
 Off. of Pub. Affs. _____
 Off. of Prof. Resp. _____
 Rec. Mgnt. _____
 Security _____
 Training _____
 Off. of EEOA _____

Enclosures
 1 - Honorable Patrick J. Leahy
 Chairman
 Committee on the Judiciary
 United States Senate
 Washington, DC 20510
 1 - Honorable James R. Clapper
 Director of National Intelligence
 FBI ExecSec, Room 6147 (TRIM # 13/DO/4459)
 AD Kelly
 Ms. Beers
 OCA Member's Folder

MAIL ROOM



U.S. Department of Justice
Federal Bureau of Investigation

Washington, D.C. 20535-0001

December 31, 2013

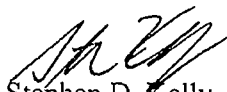
Honorable Charles E. Grassley
Ranking Member
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Senator Grassley:

This responds to your letter to Director Comey dated December 17, 2013, in which you requested copies of two training videos about the FBI's Insider Threat Program. The videos, titled Betrayed and Game of Pawns, were developed jointly by the FBI's Counterintelligence Division and the Office of the National Counterintelligence Executive (ONCIX). The videos are enclosed and are considered law enforcement sensitive for official use only, so we would request that you not disclose the videos further without contacting us.

If I can be of additional assistance in this or any other matter, please feel free to contact me at

Sincerely,


Stephen D. Kelly
Assistant Director
Office of Congressional Affairs

b6
b7c

Enclosures

- 1 - Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510
- 1 - Honorable James R. Clapper
Director of National Intelligence

December 31, 2013

Honorable Charles E. Grassley
Ranking Member
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Senator Grassley:

This responds to your letter to Director Comey dated December 17, 2013, in which you requested copies of two training videos about the FBI's Insider Threat Program. The videos, titled Betrayed and Game of Pawns, were developed jointly by the FBI's Counterintelligence Division and the Office of the National Counterintelligence Executive (ONCIX). The videos are enclosed and are considered law enforcement sensitive for official use only, so we would request that you not disclose the videos further without contacting us.

If I can be of additional assistance in this or any other matter, please feel free to contact me at

b6
b7c

Sincerely,

Stephen D. Kelly
Assistant Director
Office of Congressional Affairs

Dep. Director _____
 FAD-Adm. **Enclosures**
 FAD-C/CI _____
 FAD-Inv. _____
 FAD-Intell. _____
 FAD-IS _____
 Asst. Dir.: _____
 Adm. Serv. _____
 CIS _____
 Crim. Inv. _____
 Cyber _____
 Finance _____
 Info. Res. _____
 Inspection _____
 Inv. Tech. _____
 Laboratory _____
 Off. of Cong. Affs. _____
 Off. of the Sec'y _____
 Comm. _____
 Off. of Intell. _____
 Off. of Pub. Affs. _____
 Off. of Prof. Resp. _____
 Rec. Mgnt. _____
 Security _____
 Training _____
 Off. of EEOA _____

I - Honorable Patrick J. Leahy
 Chairman
 Committee on the Judiciary
 United States Senate
 Washington, DC 20510
 I - Honorable James R. Clapper
 Director of National Intelligence
 FBI ExecSec, Room 6147 (TRIM # 13/DO/4459)
 AD Kelly
 Ms. Beers
 OCA Member's Folder

MAIL ROOM



Congressional Affairs Office Congressional Contacts

Event Date: 6/6/2013

Classification Level: Classified

Date Entered: 06/10/2013

2013-280

Proactive

Reactive

Briefing

Hearing

SAC CV

HQ CV

FOC

Other

of SAC CV Visits: 0

Brief Type: Member

Event Date: 6/6/2013

Event Time: 12:30 PM

Entered By: [Redacted]

Unit: CLUI

Topic: Insider Threat / Bo Jiang / Shane Todd

Division: [Redacted]

OCA Contact Person: [Redacted]

DOJ Contact: [Redacted]

Date: 6/6/2013

Attended: [Redacted]

FBI Participants: UC [Redacted]
DAD Vincent Lisi
SC Mark Bartek

Other Participants: none

Committees /Subcommittees House Appropriations Subcommittee on Commerce Justice Science and Related Agencies(HAC CJS)

Members/Staff: Rep. Frank Wolf, staff [Redacted]

Executive Summary:

Insider Threat / [Redacted]

Details of Event:

On 06/06/2013 the FBI provided a classified briefing to Rep. Frank Wolf and staff: 1) Insider Threat program to

[Redacted]

Follow Up Action:

none

Attachment:

0

b6
b7C

b6
b7C

b6
b7C
b7E



Congressional Affairs Office Congressional Contacts

Event Date: 3/12/2014 Classification Level: UnClassified

Date Entered: 03/12/2014 2014-600 Proactive Reactive

Briefing Hearing SAC CV HQ CV FOC Other # of SAC CV Visits: 0

Brief Type: Event Date: 3/12/2014 Event Time:

Entered By: [Redacted] Unit: CLU II

Topic: Acknowledgement from Grassley staffer [Redacted] that he did not respond to FBI's offer more than a month ago for a briefing on the matter of Insider Threat program, and request for a briefing. Division: [Redacted]

b6
b7C

OCA Contact Person: [Redacted]

DOJ Contact: [Redacted] Date: [Redacted] Attended: [Redacted]

FBI Participants: [Redacted]

Other Participants:

Committees /Subcommittees

Members/Staff: [Redacted] Grassley staffer

b6
b7C

Executive Summary:

[Redacted] re Insider Threat program briefing

Details of Event:

Acknowledgement from Grassley staffer [Redacted] that he did not respond to FBI's offer more than a month ago for a briefing on the matter of Insider Threat program. Agent [Redacted] renewed the offer of a briefing. [Redacted] agreed. Will follow up with prospective date/time.

b6
b7C

Follow Up Action:

Attachment:

0



Congressional Affairs Office Congressional Contacts

Event Date: 3/24/2014 Classification Level: Classified

Date Entered: 04/01/2014 2014-612 Proactive Reactive

Briefing Hearing SAC CV HQ CV FOC Other # of SAC CV Visits: 0

Brief Type: Member Event Date: 3/24/2014 Event Time: 4:30 PM

Entered By: [Redacted] Unit: CLUI

Topic: HPSCI FY 2015 Budget Division: NSB

OCA Contact Person: [Redacted]

DOJ Contact: N/A Date: 4/1/2014 Attended: [Redacted]

FBI Participants: EAD McCabe

Other Participants: DHS-I&A [Redacted]

Committees /Subcommittees House Permanent Select Committee on Intelligence(HPSCI)

Members/Staff: Miller, King, Schiff, Rooney, Pompeo, Conaway, Nunes, Heck, Himes, Sewell, Bachman

Executive Summary:

Fiscal Year 2015 HPSCI Member brief on FBI budget.

Details of Event:

The brief was held at a classification level that precludes most information discussed from being entered into this log. Mr. Miller acted as Chair and opened the brief with positive remarks and praise for the FBI and a negative opening statement regarding DHS-INA past performance. He primarily wanted to hear from FBI about the state of the Insider Threat Program and current levels of resources dedicated to Cyber matters. Mr. King left the Hearing immediately following roll call and did not participate. Mr. Schiff mainly asked about FBI plans moving forward for Insider Threat, cyber and surveillance matters. Mr. Conaway asked about NSRP, surveillance capabilities, the FBI [Redacted] All of his questions were answered with no get-backs. Dr. Heck was curious about which areas the Bureau is willing to accept risk, in light of decreasing budget. No get-backs for Heck. Ms. Bachman's only questions were about FBI linguists and were answered to her apparent satisfaction. No get-backs for Bachman. More details are included in the TS/SCI level IMS.

Follow Up Action:

For Mr. Miller- Are all FBI computers, both NIP and non-NIP, auditable? [Redacted] advised he would provide answer after confirming. For Mr. Schiff-Wants specific percentage of FBI CT work both before and after 9/11. [Redacted] advised he would get actual numbers.

Attachment:

0

b6
b7C

b6
b7C

b7E

b6
b7C



Congressional Affairs Office Congressional Contacts

Event Date: 4/4/2014 Classification Level: UnClassified

Date Entered: 05/29/2014 2014-698 Proactive Reactive

Briefing Hearing SAC CV HQ CV FOC Other # of SAC CV Visits: 0

Brief Type: Event Date: 4/4/2014 Event Time:

Entered By: [Redacted] Unit: CLU II

Topic: Briefing for Grassley staffers regarding FBI Insider Threat Program Division: [Redacted]

b6
b7C

OCA Contact Person: [Redacted]

DOJ Contact: [Redacted] Date: [Redacted] Attended: [Redacted]

FBI UC Participants: [Redacted]

Other Participants:

Committees
/Subcommittees

Members/Staff: [Redacted]

b6
b7C

Executive Summary:

Briefing for Grassley staffers regarding FBI Insider Threat Program

Details of Event:

Briefing for Grassley staffers regarding FBI Insider Threat Program. This briefing was coordinated in advance with staffer [Redacted] who requested a briefing specifically on the FBI Insider Threat program -- no other topic was proposed or requested by [Redacted] to be briefed. After UC [Redacted] introduced himself and noted his role among other things as a [Redacted] of the Insider Threat Task Force, staffer [Redacted] opened with a remark that FBI videos did not distinguish Insider Threat from whistleblowers. Agent [Redacted] reminded staffers that FBI was there, per [Redacted] request, to brief on the topic of Insider Threat Program, and invited staffers to ask questions regarding the Insider Threat program, and noted to staffers that UC [Redacted] was not there to brief on matters regarding whistleblowing. Reference was made to a website that may provide guidance for prospective whistleblowers. UC [Redacted] noted that, as far as he knew, if someone is a whistleblower then any investigation under Insider Threat is suspended; he further noted that he was not asked or prepared to brief on whistleblowing, and was ready, willing, and able to proceed with briefing on the matter of the Insider Threat program. Staffers [Redacted] refused to keep to the subject of Insider Threat program, and instead badgered exclusively for statements regarding whistleblowing. Agent [Redacted] again reminded staffers [Redacted] and [Redacted] that they had requested only for an briefing on the Insider Threat program, and Agent [Redacted] read to the staffers the content of staffer [Redacted] email that requested a briefing only on the topic of Insider Threat program. Agent [Redacted] further told staffers that if they want a briefing in the future on whistleblowing, then they should make that request. Staffers [Redacted] and [Redacted] refused and continued their badgering with questions unrelated to the Insider Threat program. Grassley staffer [Redacted] continued bad faith rendered the purpose of the instant briefing null, and FBI departed.

b6
b7C

Follow Up Action:

Attachment:

0



Congressional Affairs Office Congressional Contacts

Event Date: 3/24/2011 Classification Level: ~~Classified~~

Date Entered: 03/25/2011 2011-96 Proactive Reactive

Briefing Hearing SAC CV HQ CV FOC Other # of SAC CV Visits: 0

Brief Type: Event Date: 3/24/2011 Event Time:

Entered By: [Redacted] Unit: CLUI

Topic: Senate Appropriations/Commerce, Justice, Science subcommittee staff briefing, re: FY 2012 Budget Rollout (~~classified~~) Division: FD

b6
b7C

OCA Contact Person: [Redacted]

DOJ Contact: [Redacted] Date: 3/23/2010 Attended: [Redacted]

FBI Participants: DAD Janice Lambert (FD)
[Redacted] (FD)
[Redacted] (FD)

Other Participants: N/A

Committees /Subcommittees Senate Appropriations Subcommittee on Commerce Justice Science and Related Agencies(SAC CJS)

Members/Staff: Staff [Redacted] (majority staff clerk-Sen. Mikulski)
[Redacted] (majority staff- Sen. Mikulski)

b6
b7C

Executive Summary:

Details of Event:

~~SECRET//NOFORN~~

(U) SAC/Commerce, Justice and Science (CJS) subcommittee majority staffers [Redacted] were briefed on the FBI's FY 2012 Budget request by FD's DAD and three FD/Budget staff.

b6
b7C

(U) ~~(S)~~ The briefing was very well received by the SAC/CJS staffers. The "get backs" from FD to the staffers include the following: justification information on the construction base figures, including the shortfalls [Redacted] construction cuts; a "cheat sheet" version of budget figures for Sen. Mikulski's use; information on the "Insider Threat" portion of the Foreign Intelligence budget, i.e., is it a new initiative or included in the base funding figures; a request for a demonstration of the new [Redacted] in an unclassified version of the PPT presentation used for the briefing; and, a request for a briefing on the proposed closure of several Resident Agencies (RA's), as well as a map of the FBI's Field Offices. ~~SECRET//NOFORN~~

b7E

Follow Up Action:

1- Justification information on the construction base figures, including the shortfalls [Redacted] construction cuts; 2- a "cheat sheet" version of budget figures for Sen. Mikulski's use; information on the "Insider Threat" portion of the Foreign Intelligence budget, i.e., is it a new initiative or included in the base funding figures; 3- a request for a demonstration of the new [Redacted] 4- an unclassified version of the PPT presentation used for the briefing; and, 5- a request for a briefing on the proposed closure of several Resident Agencies (RA's), as well as a map of the FBI's Field Offices.

b7E

Attachment:



Congressional Affairs Office Congressional Contacts

Event Date: 5/25/2011 Classification Level: Unclassified

Date Entered: 05/27/2011 2011-244 Proactive Reactive

Briefing Hearing SAC CV HQ CV FOC Other # of SAC CV Visits: 10

Brief Type: _____ Event Date: 5/25/2011 Event Time: _____

Entered By: [Redacted] Unit: CLU II

Topic: Boston SAC Richard DesLauriers Courtesy Visits - Day 2 of 2 Division: _____

OCA Contact Person: [Redacted]

DOJ Contact: N/A Date: _____ Attended: _____

FBI Participants: Boston SAC Richard DesLauriers

Other Participants: None

Committees
/Subcommittees

Members/Staff: Rep Michaud (D - 2nd ME) [Redacted]; Rep Keating (D - 10th MA) [Redacted]; Senator Ayotte (NH) [Redacted]; Rep Langevin (D - 2nd RI) [Redacted]; Rep Keating (D - 10th MA) [Redacted]; Rep Olver (D - 1st MA) [Redacted]; Sen Scott Brown (MA) [Redacted]; Sen J. Reed (RI) [Redacted]; Sen Whitehouse (RI) [Redacted]; Sen John Kerry (MA) [Redacted]; (D - 3rd MA) [Redacted]

Executive Summary:

Details of Event:

SAC DesLauriers conducted courtesy visits with the following Representatives, Senators and their corresponding staff: Rep Michaud (D - 2nd ME) [Redacted]; Rep Keating (D - 10th MA)/Garret [Redacted]; Senator Ayotte (NH)/Samantha Roberts & John Lawrence; Rep Langevin (D - 2nd RI)/Davis Hake & Christopher [Redacted]; Rep Keating (D - 10th MA) [Redacted]; Rep Olver (D - 1st MA) [Redacted]; Sen Scott Brown (MA) [Redacted]; Sen J. Reed (RI) [Redacted]; Sen Whitehouse (RI) [Redacted]; Sen John Kerry (MA) [Redacted]; Rep McGovern (D - 3rd MA) [Redacted]; Rep Michaud requested that the SAC consult with Maine's US Attorney to review the State's report following an officer-involved shooting at a VA hospital which resulted in the death of one of Rep Michaud's constituents (constituent's family, also constituents, are petitioning for a federal review). It was fun to note that Rep Keating's office was once occupied by John F. Kennedy. Senator Ayotte was extremely supportive of the FBI and very knowledgeable about FBI-related issues (such as the Patriot Act). She expressed strong support to help the FBI achieve its mission. She mentioned a visit she had earlier in the day with an executive with Microsoft who explained to her that Microsoft has developed a new imaging technology that could be used to combat child pornography. Microsoft would like to offer this software to the federal government for free if they feel it could be helpful. Sen Ayotte's office provided the following contact information at Microsoft for follow-up: [Redacted] Microsoft Federal Government Affairs [Redacted] [Redacted] microsoft.com. Rep Langevin mentioned that his career aspiration as a young man before his accident was to become an FBI Agent. His staffers had follow-up issues regarding Cyber threats and Cyber security. Specifically mentioned was the recent Cyber IG report that was critical of the FBI, yet the staffers' interaction with the private sector implied great confidence in the FBI's abilities to investigate intrusions. The other staffer [Redacted] wanted to know what more the FBI is doing or could do to prevent future problems like "Wikileaks". They requested a "get back" regarding the National Insider Threat Program and SAC DesLauriers mentioned that [Redacted] might be good choices for that. Sen Whitehouse mentioned that he will be sponsoring legislation with Sen Kyl addressing "Cyber Security Public Awareness" and wanted to know more about what the FBI does in that arena. Sen Whitehouse's biggest concern right now is that when someone becomes a victim online (e-mail, Internet, etc.) they don't know where to turn for help. Sen Whitehouse wants to make sure that the government has solutions to offer the public when they find themselves as online victims AND he wants the public to know (public awareness campaign) immediately where they should turn to find that help. All visits were friendly and pleasant. Attempts to set up appointments for SAC DesLauriers with Representatives Neal (D - 2nd MA) [Redacted] (D - 8th MA) [Redacted] (D - 1st ME) [Redacted] (R - 1st NH) and Senators Snowe (ME) and

b6
b7C

b6
b7C

b6
b7C



Congressional Affairs Office Congressional Contacts

Shaheen (NH) were unsuccessful. Rep Frank (D - 4th MA) declined an invitation to meet with SAC DesLauriers in D.C. because they have met each other on several occasions previously.

Follow Up Action:

None.

Attachment:

0



Congressional Affairs Office Congressional Contacts

Event Date: 8/1/2011 Classification Level: Classified

Date Entered: 08/12/2011 2011-341 Proactive Reactive

Briefing Hearing SAC CV HQ CV FOC Other # of SAC CV Visits: 0

Brief Type: _____ Event Date: 8/1/2011 Event Time: _____

Entered By: _____ Unit: CLUI

Topic: Insider Threat Study Division: SECD

OCA Contact Person: _____

DOJ Contact: _____ Date: 7/27/2011 Attended: _____

FBI Participants: UC _____ SC Patrick Reidy

Other Participants: None

Committees /Subcommittees: Senate Select Committee on Intelligence(SSCI)

Members/Staff: _____

Executive Summary:

Details of Event:

(U) The brief was requested by staff _____ as part of the Insider Threat Study being conducted by the Audit and Oversight Staff of the SSCI.

(U) ~~(S)~~ UC _____ provided a comprehensive overview of the Enterprise Security Operations Center's (ESOC) programs and capabilities of detecting and recording unauthorized access to the computer systems of the FBI. The programs used and future plans for the ESOC to address the insider threat were discussed. Cooperation and interaction within the FBI and the intelligence community were described.

Follow Up Action:

(U) Staff requested the Circular number for one OMB circular regarding encryption

Attachment:

0

b6
b7C

b6
b7C

b6
b7C

b6
b7C



Congressional Affairs Office Congressional Contacts

Event Date: 8/2/2011 Classification Level: Classified

Date Entered: 08/12/2011 2011-340 Proactive Reactive

Briefing Hearing SAC CV HQ CV FOC Other # of SAC CV Visits: 0

Brief Type: Staff Event Date: 8/2/2011 Event Time:

Entered By: Unit: CLUI

Topic: Insider Threat Study Division: CD

OCA Contact Person:

DOJ Contact: Date: 7/27/2011 Attended:

FBI Participants: SC Randall Coleman, ASC UC

Other Participants: None

Committees /Subcommittees Senate Select Committee on Intelligence(SSCI)

Members/Staff:

Executive Summary:

Details of Event:

(U) The brief was requested by staffer as part of the Insider Threat Study being conducted by the Audit and Oversight Staff of the SSCI.

(S) SC Coleman outlined the Counter Intelligence Division's (CD) approach to combating the insider threat problem, both within the FBI and the intelligence community (IC) as a whole. He discussed the outreach and education program including the use of the movie "Betrayed" and training programs. The cooperation between agencies in prevention, deterrence and investigation was described. Coleman also detailed the CD's role in carrying out investigations of unauthorized disclosure and espionage throughout the IC. The staff asked a variety of questions relating to the topic.

Follow Up Action:

(U) Staff requested the statutory language relating to a \$500,000 reward for information leading to arrests in counter intelligence investigations. They also requested the working title to an Executive Order relating to Insider Threat.

Attachment:

0

b6
b7C

b6
b7C

b6
b7C



Congressional Affairs Office Congressional Contacts

Event Date: 8/31/2011 Classification Level: UnClassified

Date Entered: 09/01/2011 2011-365 Proactive Reactive

Briefing Hearing SAC CV HQ CV FOC Other # of SAC CV Visits: 0

Brief Type: Event Date: 8/31/2011 Event Time:

Entered By: BEERS, ELIZABETH Unit: FO

Topic: Senator Johnson staff visit to FBI Milwaukee Division: FD

OCA Contact Person: BEERS, ELIZABETH

DOJ Contact: none Date: Attended:

FBI Participants: SAC Nancy McNamera

Other Participants: None

Committees /Subcommittees Senate Appropriations Subcommittee on Commerce Justice Science and Related Agencies(SAC CJS)

Members/Staff: []

b6
b7C

Executive Summary:

Details of Event:

Staffer requested support from Finance Division to stop by the MW FO during a scheduled visit to the state. [] staffs Sen. Johnson (R-WI) who sits on our appropriations subcommittee. SAC McNamera met with the staffer and provided a backbrief to OCA. Overall, [] message was that the Senator is very supportive of the FBI's mission and wants to restore any funds that the FBI is slated to lose. However, the Senator is also concerned about overlapping missions throughout the USG. In addition, he is interested in Cyber and whether is USG is efficiently meeting that mission requirement. SAC McNamera highlighted three issues that she briefed: 1) responding to Cyber concerns, SAC focused on the insider threat issue and everything that the FBI is doing to lock down our systems and address vulnerabilities. She is going to talk with CD DAD Anderson about providing the staffer with a copy of the movie "Betrayed" produced by CD. 2) SAC spoke specifically about cost savings measures in MW - i.e. they've parked cars. She also talked about the RA closings and how, more than just saving rent money, it's about gaining efficiencies via the consolidation. 3) Finally, they talked about HIDTA and the SAC advised [] that based on her experience in MW, it is an area where there may be some mission overlap. She was clear to say that she didn't speak for the HIDTA program, but only about her experience in MW.

b6
b7C

Follow Up Action:

None.

Attachment:

0



Congressional Affairs Office Congressional Contacts

Event Date: 11/16/2011 Classification Level: UnClassified

Date Entered: 11/17/2011 2011-479 Proactive Reactive

Briefing Hearing SAC CV HQ CV FOC Other # of SAC CV Visits: 0

Brief Type: Staff Event Date: 11/16/2011 Event Time: 10:00 AM

Entered By: [Redacted] Unit: CLU II

Topic: Congressional staff visit to Defense Security Service Division: [Redacted]

OCA Contact Person: [Redacted]

DOJ Contact: [Redacted] Date: 11/10/2011 Attended: [Redacted]

FBI Participants: FBI-Phila; SA [Redacted]
SA [Redacted]

Other Participants: Defense Security Service staff; Center for Development of Security Excellence (CDSE)

Committees /Subcommittees Other

Members/Staff: Staff for:
Sen. Chris Coons
Sen. Frank Lautenberg
Rep. Frank LoBiando

Executive Summary:

FBI Phila participated in a DSS presentation on insider threats and defensive briefing for govt contractors and Congressional staffers.

Details of Event:

SA [Redacted] and SA [Redacted] introduced FBI video "Betrayed", followed by slides about most significant threats to information and security faced by government contractors and personnel.

Follow Up Action:

None

Attachment:

b6
b7C

b6
b7C

CQ CONGRESSIONAL TRANSCRIPTS
Congressional Hearings
Feb. 10, 2011 - Final

House Select Intelligence Committee Holds Hearing on Worldwide Threats

ROGERS:

We'll call the committee and we'll come to order.

I want to welcome Director Clapper and our other witnesses this morning. They are very busy people.

And I appreciate you all taking the time today away from that important work from your agencies to participate in today's hearing.

Please pass along our thanks and appreciation to the men and women in your agency for their commitment and dedication in the defense of the United States. We are eternally grateful for their sacrifices.

I also want to welcome Dutch Ruppertsberger as the committee's new ranking member. He is a solid leader. His dedication and talent will serve the committee and country well.

Dutch is also a friend, and I look forward to working with him to foster the strong bipartisan energy that we're going to need to lead this committee to our oversight responsibilities and to keep America safe. And of course it never hurts to have a former prosecutor on your side.

I'm looking forward to the discussion of threats in the witnesses' statements this morning, and the questions and answers that follow.

Before we get to that, I want to talk a moment about where I would like the committee to go in the new Congress. And we've had the opportunity to talk with each of you about that direction, from reasserting oversight to taking a strong evaluation of the 10 years where the budget has grown exponentially and changed significantly; the budget, cyber issues, leaks and many others.

On reasserting oversight, it's a profound honor and a tremendous responsibility to assume the role of the HPSCI chairman in such an important juncture in our nation's history.

The U.S. intelligence community is vital to defending our nation from many threats that we face. I have no doubt that the hard work of our intelligence professional is one of the primary reasons there has not been a successful major attack in the homeland since 9/11, despite numerous failed and disrupted plots and Al Qaida's unrelenting efforts to attack the United States.

I don't believe it's been deployed on every node, but I will get back to you on that for the record, sir.

LANGEVIN:

Director Mueller?

MUELLER:

I would say that what has been in place for a couple of years it called the National Cyber Investigative Joint Task Force, is a hub of identifying an early -- attributing attacks, big, larger or small. You have all of the relevant agencies there and the expertise and the tie-in into the relevant agencies.

If it -- if it turns out to be an attack by your -- your high school student down the street, then we obviously would take it'd be a crime. More particularly that, it goes to the question of stopping an attack, depending on the -- from whence the attack originates, you would have people at the table there who have the capability of doing it. If it originates overseas, certainly NSA, CIA, and others. If it originates in the United States, we would have jurisdiction. If it comes to the -- in putting a wall on between the attackers and particular entities within the United States, DHS would have a role.

But we have a focal point that identifies immediately the attack and then immediately tries to deterring the focus of that -- that attack and utilize all of the capabilities we have to address it, regardless of whether it's in the intelligence side or the -- or the law enforcement side.

LANGEVIN:

Let me turn quickly to some of the things we're talking about, especially with respect to protecting dot-mil and -- and -- and dot-gov, our perimeter defenses. What is our level of progress in being able to protect against -- and dealing with the insider threat, as it relates to cyber?

CLAPPER:

Well, that's -- that is -- that issue has -- has come to the fore and been reaffirmed by the WikiLeaks disclosures. And certainly within the intelligence community, at least, we -- we have, I think, a strategy and embarked on an improvement program to attend to the insider threat, whether it's WikiLeaks or any -- any sort of insider threat through better identification of people who are on networks, controlling movable media, and most importantly -- and this applies for -- to several purposes -- auditing and monitoring.

And we're -- our progress is uneven to this point. And we've embarked on a campaign to -- to police that up, particularly within the intelligence enterprise.

MEMORANDUM FOR THE ATTORNEY GENERAL
SUBJECT: [Illegible]

United States Senate

COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510-6275

December 17, 2013

VIA ELECTRONIC TRANSMISSION

The Honorable James B. Comey, Jr.
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, DC 20535

Dear Director Comey:

On October 28, 2013, I received a letter from the Federal Bureau of Investigation (FBI) in which it indicated that it had collaborated with the Office of the Director of National Intelligence (ODNI) on two training videos about the FBI's National Insider Threat Program. The videos, titled *Betrayed* and *Game of Pawns*, were developed jointly by the FBI's Counterintelligence Division and ODNI's Office of the National Counterintelligence Executive (ONCIX). The FBI has also produced other insider threat materials, such as the brochure, *The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy*.¹

As I understand it, the National Insider Threat Program is the result of Executive Order 13587, issued by President Obama in October 2011, which established an interagency Insider Threat Task Force, to be staffed by the FBI and the ONCIX.² It also directed Executive Branch departments and agencies to develop their own insider threat programs. The President subsequently issued a Presidential Memorandum in November 2012 transmitting the National Insider Threat Policy and setting forth minimum standards for departmental and agency programs.³

These efforts have subsequently received press attention, some of which has focused on concerns about whether the program adequately protects whistleblowers.⁴

¹ Federal Bureau of Investigation, *The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy*, http://www.fbi.gov/about-us/investigate/counterintelligence/insider_threat_brochure.

² Executive Order 13587 – Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011. Available at <http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-structural-reforms-improve-security-classified-networks->.

³ Presidential Memorandum – National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Nov. 21, 2012. Available at <http://www.whitehouse.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand>.

⁴ For example, Marisa Taylor and Jonathan S. Landay, "Obama's crackdown views leaks as aiding enemies of U.S.," *McClatchy* (Jun. 20, 2013), available at

As you know, I strongly believe that whistleblowers play an important role in safeguarding the federal government against waste, fraud, and abuse. You too stated in your confirmation hearing that you believe whistleblowers are a critical element of a functioning democracy. Their willingness to come forward contributes to improving government operations. They often put themselves at risk of reprisal from their employers, sometimes being demoted, reassigned, or fired as a result of their actions. Under the Whistleblower Protection Act and Presidential Policy Directive 19, federal employees may not be retaliated against for reporting waste, fraud, and abuse.⁵

Accordingly, some agencies have taken steps to prevent the insider threat program from chilling whistleblower communications. For example, the Office of the Inspector General for the Intelligence Community is developing training that integrates whistleblowing into the agency processes, making the Intelligence Community whistleblowing and insider threat programs mutually reinforcing.

In order to assess whether training materials on the National Insider Threat Program provide adequate guidance on protecting whistleblowers, I respectfully request that you provide me with copies of *Betrayed* and *Game of Pawns*, as well as copies of any other training materials regarding the National Insider Threat Program or any FBI-specific insider threat program. I would appreciate receiving these materials by January 14, 2014. I know that you consider transparency to be an important value, and I trust that transparency on this issue will benefit both whistleblowers and our national security.

Should you have any questions regarding this letter, please contact [redacted] of my staff at [redacted]

b6
b7c

Sincerely,



Charles E. Grassley
Ranking Member

cc: The Honorable James R. Clapper
Director of National Intelligence

~~SECRET//NOFORN~~

**Responses of the Federal Bureau of Investigation
to Questions for the Record
Arising from the April 14, 2011, Hearing Before the
House Permanent Select Committee on Intelligence
Regarding the FBI's Fiscal Year 2012 National Intelligence Program Budget**

Questions Posed by Chairman Rogers

1. How much does a surveillance team cost? Please provide the costs of various sized teams and armed vs. unarmed teams?

Response:

(U) ~~(S//NF)~~ In Fiscal Year 2011 it costs approximately [] to establish a new armed surveillance team and approximately [] to establish a new unarmed surveillance team.

b7E

(S) 2. During the hearing [] stated that the FBI can currently surveil [] targets on a 24x7 basis. What is the FBI's goal for the number of targets it is able to cover on a 24x7 basis? How many additional positions and how much additional funding would be required to meet this goal?

b1
b3

b6
b7C

Response:

(S) (U) ~~(S//NF)~~ At present, the FBI is capable of covering [] targets on a 24/7 basis. Our goal is to build a national surveillance capacity to provide for additional coverage.

b1
b3

3. The FBI requested no enhancements in FY 2012 for linguists. How does FBI plan to handle the increasing volume of documents that requires translation?

Response:

(U) The demands on the FBI's Foreign Language Program (FLP) fluctuate and priorities are adjusted frequently to meet the greatest need at any given time. The

~~SECRET//NOFORN~~

These responses are current as of 7/22/11

(U) ~~(S//NF)~~ [redacted]
 (S) [redacted]
 (S) [redacted]
 (S) [redacted]
 [redacted]
 [redacted]

b1
b3
b7E

b. Is the FBI giving sufficient attention to other counterintelligence threats?

How so?

Response:

(U) ~~(S//NF)~~ Because the FBI's National CI Strategy prioritizes [redacted]
 [redacted] The FBI's
 [redacted]
 (S) [redacted] with appropriate attention afforded to
 [redacted]
 (S)(S) [redacted] In addition to [redacted]
 (S) [redacted] all of which are addressed in the FBI's
 [redacted]

b1
b3
b7E

5. Last year, the FBI created [redacted] Regional Intelligence Groups (RIGs) to facilitate cooperation among field offices in the same region.

b7E

a. What specific value-added have the RIGs provided?

Response:

The FBI continually recruits for all necessary languages, and attempts to address all work possible. The chart provided as Enclosure A reflects the hiring in recent years up to 12/31/06 in the critical counterterrorism languages. When the FBI does not have the language resources for a particularly rare language, we work with contractors and with the National Virtual Translation Center (NVTC) to address those needs. In one situation, the FBI used Department of Defense (DoD) contracts to provide cross-training for FBI Arabic linguists on an unusual dialect of Arabic that was needed. These resources provide a surge capacity in the FBI=s most critically needed languages as well as a pool of linguists in less commonly needed languages that are important to the FBI=s mission. Contract linguists must pass the same language test batteries and security vetting as full-time employees. Their Top Secret clearances, native-level proficiency in the foreign language, high-level of skill in English, and knowledge of the target culture make FBI contract linguists a highly desirable commodity in the IC. Many of the FBI=s contract linguists provide support in languages that the full-time linguist staff does not cover. The FBI depends on the contract linguists and NVTC for a substantial amount of the needed support in many languages critical to the FBI=s mission.

While the FBI continues to hire new contract linguists, it is currently converting many of the talented contract linguists hired since 9/11/01 to full-time language analysts, with the goal of maintaining a language workforce composed of one-third contract linguists and two-thirds FBI language analysts. This ratio will enable the FBI to maintain a stable workforce and will provide greater job security and benefits for the linguists proficient in the languages most needed to meet ongoing national security requirements.

Since May 2006, the FBI has made a special effort to focus on the backlog and has decreased the unaddressed counterterrorism work in the most critical languages to less than 1,000 hours. While the figures referenced in the May 2006 hearing pertain to counterterrorism cases only, audio backlog continues to be a concern for the FBI. In general, audio collection in the difficult and unusual languages represents only about 1% of the FBI=s total audio collection in the past four years.

WHISTLEBLOWERS

17. Whistleblower Mike German has alleged that the FBI failed to investigate a potential terrorist link between white supremacist and Islamic extremists. During our investigation of this case, our staff received two different versions of a crucial transcript. Neither version of this transcript was complete.

These responses are current as of 2/8/07

a. Can you explain the apparent discrepancies in the two versions of the transcript?

Response:

In connection with its investigation of this matter, by letter dated 2/3/06 the Committee requested from the DOJ OIG copies of documents the OIG relied upon in preparing its reports. The document request included the transcript of the 1/23/02 tape-recorded meeting between members of the foreign and domestic terrorist groups, which German had provided to the OIG in February 2003, and any other transcripts made of that meeting. By letter dated 7/27/06, the FBI provided the Committee with copies of the FBI documents responsive to this request, including copies of two transcripts of the 1/23/02 meeting.

One version of the transcript, identified with the text marking A037eb01.t3@ at the top left of each page, was obtained from German on 2/12/03 during his interview by investigators from DOJ=s OIG and FBI. German produced and referenced portions of this transcript in support of information he provided in his signed, sworn statement, and this version was attached to and made a permanent part of German=s sworn statement. This version of the transcript is a rough draft of the transcription of a consensually monitored conversation that occurred on 1/23/02; it contains several instances of Aunintelligible@ conversations on the recording and abruptly ends on page 126. On page 49, the construction of this document changes from a rough draft format to FBI FD-302a format, and continues sequentially but displays the page number starting at 46. This Acombination@ document submitted by German contains duplicative pages of the rough transcription and the FD-302a, so that pages 46, 47, 48, and 49 are misnumbered yet sequential. It is unknown why German provided to OIG and FBI interviewers only 126 pages of a total 167 pages or why this document has a combination of transcript formats.

The second version of the transcript, identified with the marking AFD-302a@ at the top left of each page, represents the draft of the entire transcription in the official FD-302a format. Because the header and footer on each page of an FD-302a reduce the remaining printing surface, the pages of this FD-302a draft do not line up exactly with the pages of the rough draft portion of the version obtained from German. In the FD-302a draft, many, though not all, of the Aunintelligible@ portions that appear in the rough draft have been clarified. This FD-302a version is a complete transcription of the 1/23/02 conversation at 167 pages, or 31 pages more than the version provided by German.

These responses are current as of 2/8/07

b. Which of the two transcripts do you consider most accurate?

Response:

For the reasons discussed above, the version identified with the FD-302a marking at the top left of each page is the most accurate.

c. Will you provide the committee with the tape that this transcript is based on, in its complete form? If not, why not?

Response:

The Committee has not previously requested a copy of the tape in connection with its oversight investigation of this matter. Should we receive a Committee oversight request from the Chairman regarding this matter, we would be pleased to consult with DOJ as to the appropriate response.

Questions Posed by Senator Grassley

AMERITHRAX INVESTIGATION

18. a. Why was Richard Lambert removed as the head of the Amerithrax investigation?

Response:

Richard Lambert served as the Inspector in Charge of the Amerithrax investigation from 9/20/02 to 9/16/06. On 5/22/06, he applied for promotion to the position of Special Agent in Charge (SAC) of the FBI's Knoxville Division. The Senior Executive Career Board reviewed the qualifications of the interested candidates and recommended Richard Lambert for selection. On 6/16/06, Director Mueller announced the selection of Mr. Lambert as the Knoxville SAC.

b. Was it related in any way to disagreements between him and others working on the investigation about the proper scope and focus of the FBI's inquiry? If so, please explain.

Response:

Mr. Lambert applied for and was selected as Knoxville SAC based on his qualifications for the position.

These responses are current as of 2/8/07.

and effectively collecting, sorting, and examining relevant data, the FBI will be able to rapidly identify indicators of misuse and other inappropriate activity. Along with these technology-driven innovations, the FBI will continue to use regular personnel reinvestigations, including reviews of employees' financial circumstances, to detect willful and/or potentially criminal misconduct.

d. What guidelines and training govern how agents deal with potential informants who may be engaged in trading or short-selling securities or may be selling information to hedge funds?

Response:

The FBI has instituted a new comprehensive informant validation process for use by field offices and FBIHQ. The validation process includes quarterly SSA reports addressing the sources' motivation, access, timeliness, corroboration, and history. As discussed above, AG Guidelines address unauthorized criminal activity by confidential sources. These AG Guidelines are covered in the New Agent core-training received at the FBI Academy and reinforced through regular legal training provided in field offices during the remainder of an SA's career.

e. In October of this year, a former FBI agent Jeffrey A. Royer was sentenced to six years in prison for racketeering and securities fraud. According to witnesses at trial, the agent provided non-public FBI information to an outside party who used the information to spread negative publicity about companies and profit from short-selling their stock. What lessons can the FBI learn from this case?

Response:

In response to a recommendation in the March 2002 Webster Commission report, the FBI's Security Division (SecD) developed and implemented a comprehensive security awareness, education, and training program for all persons with access to FBI information. This comprehensive approach included the development of a professional cadre of highly trained Chief Security Officers, who now provide FBI personnel with the most up-to-date security policy, training, lessons learned, and best practices.

SecD uses a variety of educational methods, to include formal classroom training, web-based training, written guidance, and mentoring, to enhance the security awareness and education of the entire FBI population. Formal classroom instruction has included: the authorized procedures for releasing information to

These responses are current as of 2/8/07

the public; refresher courses on establishing an information recipient's "need-to-know"; and the potential penalties for deviating from established procedures. Instruction is also provided in the form of ANon-disclosure and Releasability briefings,@ during which all personnel execute a "Classified Information Non-disclosure Agreement" and "FBI Rules of Behavior" form acknowledging their responsibility to protect and properly handle FBI information. SecD also provides a host of additional training opportunities and materials, each of which serves to reinforce security awareness throughout the FBI.

While this approach will not stop a trusted insider intent on disclosing information for improper purposes, it ensures the employee is educated on proper information handling techniques and encourages each employee to report others who violate the rules. In other words, FBI employees now better understand their role in protecting and ensuring the security of FBI information, personnel, and facilities.

f. What safeguards exist to prevent agents like Royer from similarly profiting on non-public information about ongoing investigations?

Response:

Please see our responses to subparts c and e, above.

USE OF GOVERNMENT-OWNED OR LEASED AIRCRAFT

36. I understand that the FBI operates a number of executive jets as part of its aviation program for both operational use and for official travel by senior FBI officials.

a. Please identify the number, type, and cost of aircraft owned and/or leased by the FBI and used for both operational purposes and travel by senior FBI officials.

Response:

The FBI reads this question as distinguishing between aircraft used to meet Amission requirements@ of the FBI and those used for the Aofficial travel@ of A senior Federal officials@ in the FBI other than to meet mission requirements, as those terms are defined in OMB Circular No. A-126.¹ While the vast majority of

¹ Paragraph 5 of OMB Circular No. A-126 (5/22/92) includes the following definitions:

b. Mission requirements means activities that constitute the

These responses are current as of 2/8/07

investigative files implicates significant individual privacy interests because these files discuss allegations against individuals under investigation. DOJ has consistently offered to accommodate Congressional requests for information about OPR investigations through briefings, minimizing the intrusion on the privacy of Executive Branch employees.

On 6/21/06 the FBI responded to the Committee's 5/10/06 request for information and documents relating to the FBI's investigation of the suspected murder of Assistant United States Attorney Jonathan Luna. In its response, the FBI advised the Committee that documents concerning OPR matters raise serious privacy considerations, particularly when, as in that instance, there was no finding of misconduct. Consistent with the policy articulated above, Candice Will, AD of the FBI's OPR, provided a 6/30/06 staff briefing that included an overview of OPR's investigation and addressed both the issues raised in the Committee's 5/10/06 letter and all issues raised by the staff. In response to a question from staff concerning the availability of the OPR report, our records reflect that AD Will did not indicate that she had no objection to producing the report, but rather advised that privacy concerns counseled against providing that document to the Committee.

FBI WHISTLEBLOWERS

42. In May, 2006, I asked the FBI for a description of each instance where an FBI supervisor has been disciplined for retaliating against a whistleblower. Two weeks ago, I received a response from your agency advising me that since 1999 no FBI supervisors have been disciplined as a result of their having retaliated against whistleblowers.

a. Why haven't any FBI supervisors been disciplined for having retaliated against whistleblowers?

Response:

As the FBI has previously indicated in response to Questions for the Record, an Assistant Special Agent in Charge (ASAC) was disciplined for whistleblower retaliation. While that sanction, which was imposed before implementation of the Bell Colwell recommendations, was ultimately vacated on appeal, that case does not indicate that supervisors are not disciplined for retaliation, but instead indicates that the FBI has procedures in place designed to protect the rights of all employees. Since that response, no allegations of whistleblower retaliation have reached final adjudication.

These responses are current as of 2/8/07

b. The DOJ/IG found that Jorge Martinez retaliated against Michael German for protected whistle blowing activity. Has FBI disciplined Martinez? If not, why not?

Response:

The FBI is well aware of this matter and is in the process of taking appropriate action. Consistent with longstanding Executive Branch policy, our goal in all cases is to satisfy legitimate oversight interests while protecting significant Executive Branch confidentiality interests. As a general matter, the disclosure of information from OPR investigative files implicates significant individual privacy interests because these files discuss allegations against individuals under investigation.

c. Since 1999, how many FBI personnel have claimed whistleblower status? How many have claimed retaliation for protected whistleblowing activity?

Response:

The FBI is not in a position to provide this information. Pursuant to 5 U.S.C. ' 2303 and 28 C.F.R. Part 27, DOJ=s OIG and OPR serve as Investigative and/or Conducting Offices in FBI whistleblower cases, while the Director of DOJ=s Office of Attorney Recruitment and Management (OARM) is authorized to adjudicate claims of FBI whistleblower reprisal and to order corrective action subject to appeal to the Deputy Attorney General (DAG). Pursuant to 28 C.F.R. ' 27.4, the identity of employees who make those claims is not disclosed to the FBI unless there is a recommendation for corrective action.

DOJ=s OARM advises that, based on numbers collectively reported by OARM, OIG, and OPR for calendar years 1999 through 2006, 96 FBI personnel have made allegations of retaliation for claimed protected whistleblowing activity. It is the FBI=s understanding that there is no formalized consolidated record of those who may initially claim whistleblower status because, in the absence of subsequent retaliation based on the whistleblowing, the mere status as a whistleblower does not affect the employees= rights or benefits.

REPORTING OF DRUG SEIZURE STATISTICS

43. The staff of the House Committee on Homeland Security, Subcommittee on Investigations, recently released a staff report entitled, AA Line in the Sand: Confronting the Threat at the Southwest Border.@ This report describes, among other things, the

These responses are current as of 2/8/07

NICS developers are receiving daily system logs for further analysis. In addition, the FBI is working in the non-operational environment in an attempt to recreate the outage, but to date these efforts have been unsuccessful.

Absent a clear indication of the cause of the outage, the only changes made to NICS as a result of it have been an increase in the shared memory pool and Oracle database cache, which appear to have resolved the issue. The FBI=s CJIS Division will continue to monitor and analyze the NICS in order to prevent or minimize future outages.

b. Does the FBI know how many gun sales were completed without background checks while the system was down?

Response:

The outage on Sunday, 11/26/06, lasted 45 minutes, and the three outages on Monday, 11/27/06, lasted 34 minutes, 1 hour 24 minutes, and 35 minutes. Even with these outages, NICS processed 17,983 firearms transactions on Sunday (11/26) and 29,867 on Monday (11/27). For comparison purposes, on the Sunday and Monday after Thanksgiving in 2005, NICS processed 14,574 and 28,200 firearms transactions, respectively. The FBI has no reason to believe gun sales were executed during the outage in violation of the legal requirements of the Brady Handgun Violence Prevention Act of 1993.

c. What is the FBI doing to make sure that this problem never happens again?

Response:

The FBI=s CJIS Division has made all of the changes recommended by the vendors. As indicated in response to subpart a, above, the problem has not recurred, but the CJIS Division will continue to monitor the system and make any corrections we identify.

MIKE GERMAN / WHISTLEBLOWERS

76. According to the Office of the Special Counsel (AOSC@), the average number of whistleblowers who have filed complaints with the government has increased by 43% since September 11, 2001. Yet, sadly, the number of whistleblowers who have filed reprisal

These responses are current as of 2/8/07

complaints with the OSC because their employers have retaliated against them for coming forward has also increased by 21% during the same time period. For example, former FBI special agent Michael German has said that his reputation and career were ruined after he reported concerns about misconduct on the Bureau's terrorism investigations to his superiors. What is the Bureau doing to protect the rights of whistleblowers within the FBI to come forward and disclose government fraud, waste and abuse?

Response:

Although the FBI can never completely eliminate an employee's fear of whistleblower retaliation, factors likely to induce such fear can be reduced or eliminated. The anonymous nature of inspection leadership surveys (which are conducted prior to internal FBI inspections to assess management effectiveness), private interviews with the inspection staff during these inspections, and executive managers who promote the proper environment all help to reduce the fear of whistleblower retaliation. If an employee nonetheless believes retaliation has occurred, this may be reported to the Inspection Division's IIS or to DOJ's OIG or OPR. FBI employees are also frequently reminded through FBI-wide emails and other mechanisms that there is a procedure established under law (5 U.S.C. ' 2303) and implemented by regulation (28 C.F.R. Part 27) that provides a formal avenue for an employee to seek corrective action based on a personnel action taken in reprisal for whistle blowing.

77. Many whistleblowers in the intelligence community are discouraged from coming forward because intelligence agencies are exempted from the Whistleblower Protection Act. Would you support legislation to extend whistleblower protections to national security employees?

Response:

Congress specifically excluded the FBI and other IC agencies from the application of 5 U.S.C. ' 2302 (the government-wide Whistleblower Protection Act) because of the classified and sensitive nature of their work and the fact that any employee may have access to such information. The legislative history indicates that the exceptions for the FBI and the other specified agencies is tied to the intelligence aspect of their missions. See H.R. Rep. 328, 101st Cong., 1989 WL 225002 (Leg. Hist.). We support the Congressional reasoning that underpins these exceptions.

Congress has provided separate whistleblower protections for national security employees through the IC Whistleblower Protection Act of 1998 (ICWPA). The

These responses are current as of 2/8/07

ICWPA provides that an employee may communicate "a complaint or information with respect to an urgent concern" regarding intelligence activities to the appropriate Inspector General (or designee) and thereafter, under specified circumstances, "to Congress by contacting either or both of the intelligence committees directly." Inspector General Act of 1978, 5 U.S.C. Appendix 3, ' ' 8H(a)(1) and (d).

ANTHRAX INVESTIGATION

78. The Bureau's investigation into the 2001 anthrax attacks that killed 5, infected 17 others and terrified millions of Americans is now well into its fifth year. Many believe that the investigation has gone very cold and no arrests have been made in the case.

- a. What is the current status of the anthrax investigation?
- b. Do you expect that criminal charges will be brought in the case and if so, when?
- c. You testified at the hearing that the FBI currently has 17 agents and 10 postal inspectors assigned to the anthrax investigation. Has the number of personnel dedicated to the investigation changed? Will you consider increasing the number of agents and investigators dedicated to this investigation?
- d. How much money has the FBI spent on the anthrax investigation to date?

Response to subparts a through d:

Pursuant to the longstanding DOJ policy against disclosing non-public information concerning pending law enforcement and litigation matters, we are unable to provide a response at this time.

79. A frequent criticism of the anthrax investigation is that the FBI has made a number of incorrect assumptions about the source of the anthrax and refused to heed outside expert advice in the case. Will the Bureau be open to new theories about the case and more receptive to outside expertise and criticism going forward?

Response:

Pursuant to the longstanding DOJ policy against disclosing non-public information concerning pending law enforcement and litigation matters, we are unable to provide a response at this time.

These responses are current as of 2/8/07

FBI SAs, the FIGs, FBIHQ, and DOJ will all have roles in measuring the value of a source's operation as well as managing the risks associated with using a human source. Redundancy of review will be an intentional part of the validation process, serving as a check and balance on human source activities, including authorized and any possible unauthorized criminal activities. The EAD of the FBI's NSB has approved a draft of the Validation Manual, and the FBI is moving toward implementation throughout the FBI.

116. Some critics argue that the FBI often allows agents involved in wrongdoing to quietly retire. What are you doing to ensure future accountability, since most of the FBI personnel responsible for the Leung security breach avoided negative consequences by retiring? Do you believe that the penalties described in your colloquy with Senator Grassley about the Woods allegations are consistent with the recommendations of the Inspector General in the Leung affair? If so, why?

Response:

As stated above in response to question 93, in order to ensure the accountability of agents who engage in wrongdoing and then attempt to quietly retire, the Director amended FBI policy governing the administrative inquiry process so that, notwithstanding the resignation or retirement of an employee, a disciplinary matter is completed where necessary to protect the institutional interests of the FBI. Obviously, any matters involving criminal allegations are pursued irrespective of an employee's retirement or resignation.

117. In response to a written question from Senator Grassley after our last Oversight hearing, you appear to acknowledge that no one has ever been disciplined for whistleblower retaliation under the FBI's guidelines. Is that accurate? Can you explain? What is being done to ensure that FBI whistleblowers are being protected from retaliation?

Response:

That is not accurate. As stated above in response to question 42a, the FBI has disciplined a number of employees for engaging in retaliatory behavior, including whistleblower retaliation. OPR recently suspended one supervisor for 30 days for engaging in retaliation against a whistleblower. Although not final, in another disciplinary matter, OPR has proposed the dismissal of a supervisor for retaliating against a whistleblower. In another, OPR imposed a 3-day suspension on a supervisor who threatened to retaliate against a whistleblower.

These responses are current as of 2/8/07

118. You also noted that, in the one FBI case where a 3-day suspension was initially imposed for whistleblower retaliation, that decision was later reversed, through an appellate process that the FBI's General Counsel declared to be flawed. What has been done to fix the appellate process?

Response:

Upon the completion of the Bell/Colwell Commission's study of the FBI's disciplinary process, the FBI adopted changes recommended by the Commission to improve the FBI's disciplinary process. With respect to the FBI's appellate process specifically, the Commission recommended key changes designed to improve the transparency and fundamental fairness of the appellate process for all FBI employees. These changes were adopted and made effective by the FBI Director on 8/19/05.

One such improvement offers non-SES employees the option to choose a mid-level manager, rather than an SES employee, to participate on the three-member Disciplinary Review Board (DRB), which convenes to hear appeals in those cases in which an adverse disciplinary sanction has been imposed by the FBI's OPR. (Previously, the voting members of the DRB's were composed strictly of SES employees.) The advantage of this change is that non-SES employees are now being judged with input from "one of their own." This concept is especially important in light of past OIG investigations into allegations of disparate treatment in the FBI's disciplinary process.

Another important change, recommended by the Commission and adopted by the FBI Director, was elimination of the ability to increase a disciplinary penalty on appeal. This change was made to ensure all employees could take full advantage of the FBI's appellate process without fear of facing additional sanctions. In addition, the Commission recommended that the "de novo" appellate standard be replaced with a "substantial evidence" standard, which is now being used to review matters on appeal. This change allows the FBI's appellate authority to continue to serve as an important check and balance on the entire OPR process.

In addition to the improvements mentioned above, the FBI's appellate authority will continue to seek the advice of the FBI's OGC when guidance is needed on legal matters. The FBI is dedicated to ensuring the FBI's appellate process continues to operate in a fair, effective, and efficient manner for all employees.

Background: In response to questions following the last FBI Oversight hearing about press reports relating to the New York Field Office, you seem to acknowledge that there may be

These responses are current as of 2/8/07

United States Senate

January 28, 2014

The Honorable Eric Holder
Office of the Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Dear Attorney General Holder:

It has now been over 15 months since the issuance of Presidential Policy Directive 19 (PPD-19). This directive mandated that the Attorney General deliver a report to the President within 180 days to assess the efficacy of the Department regulations that implement the Whistleblower Protection Act ("WPA") for Federal Bureau of Investigation (FBI) employees.

Specifically, the provision states:

Within 180 days of the date of this directive, the Attorney General, in consultation with the Special Counsel and Federal Bureau of Investigation employees, shall deliver a report to the President that assesses the efficacy of the provisions contained in part 27 of title 28, Code of Federal Regulations in deterring the personnel practices prohibited in section 2303 of title 5, United States Code, and ensuring appropriate enforcement of that section, and describes any proposed revisions to the provisions contained in Part 27 of title 28 that would increase their effectiveness in fulfilling the purposes of section 2303 of title 5, United States Code.¹

This report was due by April 8, 2013. However, to date, there has been no public announcement that the review has been completed. The report appears to be nearly ten months overdue.

A comprehensive review is vital to correct the shortcomings of the FBI whistleblower process. For years, I have asked the FBI about whistleblowers such as [redacted]. On March 15, 2007, the Department's Office of Inspector General found that [redacted] was retaliated against for pointing out fraudulent activities in the FBI. The FBI appealed the Inspector General's findings to Main Justice's Office of Attorney Recruitment and Management [OARM]. In 2009 and 2010, I asked you about [redacted] and the extremely lengthy amount of time OARM takes to make decisions. In response to one of those questions, you replied on March 22, 2010: "OARM has been

¹ Presidential Policy Directive/PPD-19, Section E, p. 5 (Oct. 10, 2012).

conducting appropriate and necessary proceedings regarding [redacted] Request for Corrective Action since it was filed in May 2006. Subject to a change in circumstances, a ruling could be issued by OARM within the next several months." Instead, OARM did not issue the final ruling until more than three years later, on July 25, 2013.

b6
b7C

[redacted] case is just one example that illustrates the dire need for a review of 28 C.F.R. Part 27 and a revision of the processes an FBI whistleblower has to follow in order to be protected. Accordingly, please answer to the following questions:

b6
b7C

1. What is the current status of your review pursuant to Section E of PPD-19?
2. Why have you failed to issue a report assessing the efficacy of 28 C.F.R. Part 27?
3. When will the report be complete?
4. When the report is complete, do you intend to provide it to the Judiciary Committee? Why or why not?

Thank you for your attention to this matter. I would appreciate a response by March 2, 2014. Should you have any questions regarding this letter, please do not hesitate to contact [redacted] of my Committee staff at [redacted] I look forward to your response.

b6
b7C

Sincerely,



Charles E. Grassley
Ranking Member

cc: The Honorable James B. Comey, Jr., Director
Federal Bureau of Investigation



Week of March 31 – April 4, 2014

Updated: March 31, 2014 (8:00 a.m.)

Date	Time	Event	Topic	FBI Participants	Other Participants	Contact
Tuesday, April 1	11:00 a.m.	HPSCI Staff Briefing	Post 9/11 Terrorism Financing	[Redacted]	TBD	[Redacted]
Friday, April 4	9:00 a.m.	HPSCI Chairman and RM Courtesy Visit	Courtesy Visit	DD Giuliano	N/A	
Friday, April 4	2:00 p.m.	Sen. Grassley Staff Briefing	National Insider Threat Program	[Redacted] CD	N/A DOJ: [Redacted]	

b6
b7C



Week of JANUARY 27 - 31, 2014

Updated: January 29, 2014 (1:00 p.m.)

Date	Time	Event	Topic	FBI Participants	Other Participants	Contact
Tuesday, January 28	8:00 a.m.	House Homeland Security Committee Member Briefing	TSC 101 and Redress Procedures/Process	PDD Steven Mabeus Director Pichota	TSA [redacted] [redacted]	[redacted]
Tuesday, January 28	9:00 a.m.	Senator Whitehouse-Guest Speaker at FBI Cyber Division All Hands Conference	The Future of Cybersecurity	DD Giuliano AD Demarest All Cyber Leadership	N/A DOJ: [redacted]	[redacted]
Wednesday, January 29	10:00 a.m.	SSCI Annual Threat Assessment Hearing	Worldwide Threats	Director Comey	DNI Clapper D/CIA Brennan DIA DOS NCTC DOJ: [redacted]	[redacted]

b6
b7C

Thursday, January 30	1:30 p.m.	Briefing to HPSCI Staff	Security Clearance, Insider Threat Reform	DAD Brooks-SecD CD-TBD	NCIX	[Redacted]
					DOJ: [Redacted]	
Thursday, January 30	4:30 p.m.	Joint SSCI HPSCI JRIG Staff Briefing	Expansion of JRIG Program	AD Velez-Villar	N/A	[Redacted]
					DOJ: [Redacted]	

b6
b7C

[Redacted] (DO) (FBI)

From: [Redacted] (CD)(FBI)
Sent: Friday, February 07, 2014 10:26 AM
To: [Redacted] (DO) (FBI)
Subject: Video Letter --- UNCLASSIFIED//~~FOUO~~
Attachments: OCA letter2.docx

SentinelCaseId: NON-RECORD

b6
b7C

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

[Redacted]

Here is the letter we'd put together on the three videos.

b6
b7C

UC [Redacted]
CD-4D

[Redacted]

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

[Redacted]

From: [Redacted]
Sent: Wednesday, February 19, 2014 3:03 PM
To: [Redacted]
Subject: Status Update re Proposed Insider Threat briefing

b6
b7C

Hi [Redacted] – I just wanted to touch base with you and let you know that we offered the briefing to Grassley staff regarding the Insider Threat program, but have not heard anything back yet; I'll let you know if they do and perhaps we can work out another date/time that will work for your schedule...

Let me know if you have any questions meantime,

Many thanks,

[Redacted]

b6
b7C

[redacted] (DO) (FBI)

From: BEERS, ELIZABETH RAE (OCA) (FBI)
Sent: Thursday, February 27, 2014 4:54 PM
To: [redacted] (DO) (FBI)
Subject: RE: New calendar item --- UNCLASSIFIED

b6
b7C

SentinelCaseId: TRANSITORY RECORD

Classification: UNCLASSIFIED

Did we ever schedule the briefing re the insider threat program?

From: [redacted] (DO) (FBI)
Sent: Thursday, February 27, 2014 4:49 PM
To: KELLY, STEPHEN (DO)(FBI); BEERS, ELIZABETH RAE (OCA) (FBI); [redacted] (DO)(FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (DO) (FBI); [redacted] (OCA) (FBI); [redacted] E (DO)(FBI); [redacted] (DO)(FBI); [redacted] (DO)(FBI); [redacted] (DO)(FBI); [redacted] (DO)(FBI); [redacted] (DO)(FBI); [redacted] (DO)(FBI); [redacted] (DO) (FBI); [redacted] (DO) (FBI); [redacted] (DO) (FBI); [redacted] (DO) (FBI); [redacted] (OCA) (FBI); [redacted] (DO) (FBI); [redacted] (DO) (FBI); [redacted] (DO) (FBI)
Subject: New calendar item --- UNCLASSIFIED

b6
b7C

Classification: UNCLASSIFIED

TRANSITORY RECORD

Calendar item:

Date and Time: March 11, 2014 at 1:30 pm
Event: Briefing
Committee/Staff: Staff for Senate Judiciary Committee
Location: TBD
Topic: Criminal History Records and Use of Non-Criminal/Justice/Civil Purposes
FBI Participants: [redacted] OGC and [redacted] CJIS
Other participants: [redacted] SEARCH
[redacted] SEARCH
[redacted] Compact Council

b6
b7C

Classification: Unclassified

OCA Contact: [redacted]
OLA Contact: [redacted]

Classification: UNCLASSIFIED

Classification: UNCLASSIFIED

[redacted] (DO) (FBI)

b6
b7C

From: [redacted] (DO) (FBI)
Sent: Friday, February 28, 2014 11:03 AM
To: BEERS, ELIZABETH RAE (OCA) (FBI)
Subject: RE: New calendar item --- UNCLASSIFIED

SentinelCaseId: TRANSITORY RECORD

Classification: UNCLASSIFIED
=====

I extended to staffer a date and time for a briefing but they have not yet responded or accepted

From: BEERS, ELIZABETH RAE (OCA) (FBI)
Sent: Thursday, February 27, 2014 4:54 PM
To: [redacted] (DO) (FBI)
Subject: RE: New calendar item --- UNCLASSIFIED

b6
b7C

Classification: UNCLASSIFIED
=====

Did we ever schedule the briefing re the insider threat program?

From: [redacted] (DO) (FBI)
Sent: Thursday, February 27, 2014 4:49 PM
To: KELLY, STEPHEN (DO)(FBI); BEERS, ELIZABETH RAE (OCA) (FBI); [redacted] (DO)(FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (DO) (FBI); [redacted] (OCA) (FBI); [redacted] (DO)(FBI); [redacted] (DO)(FBI); [redacted] (DO)(FBI); [redacted] (DO)(FBI); [redacted] (DO)(FBI); [redacted] (OCA) (FBI); [redacted] (DO) (FBI); [redacted] (DO) (FBI); [redacted] (DO) (FBI)
Subject: New calendar item --- UNCLASSIFIED

b6
b7C

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

Calendar item:

Date and Time: March 11, 2014 at 1:30 pm
Event: Briefing
Committee/Staff: Staff for Senate Judiciary Committee
Location: TBD
Topic: *Criminal History Records and Use of Non-Criminal/Justice/Civil Purposes*
FBI Participants: [redacted], OGC and [redacted] CJIS
Other participants: [redacted] SEARCH
[redacted] SEARCH
[redacted] Compact Council

b6
b7C

Classification: Unclassified

OCA Contact:

OLA Contact:

b6
b7c

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

[redacted] (DO) (FBI)

b6
b7C

From: KELLY, STEPHEN (DO)(FBI)
Sent: Tuesday, December 24, 2013 12:49 PM
To: [redacted] (CD)(FBI)
Cc: BEERS, ELIZABETH RAE (OCA) (FBI) [redacted] (DO) (FBI)
Subject: RE: Materials Responsive to Sen Grassley's Letter Re: Insider Threat ---
UNCLASSIFIED//~~FOUO~~

SentinelCaseId: NON-RECORD

Classification: UNCLASSIFIED//~~FOUO~~

Thanks [redacted]

b6
b7C

I've included Beth and [redacted], who can handle this when they return from the holidays.

Merry Christmas.

- Stephen

Stephen D. Kelly
Assistant Director
Office of Congressional Affairs

From: [redacted] (CD)(FBI)
Sent: Monday, December 23, 2013 2:04 PM
To: KELLY, STEPHEN (DO)(FBI)
Subject: Materials Responsive to Sen Grassley's Letter Re: Insider Threat --- UNCLASSIFIED//~~FOUO~~

b6
b7C

Classification: UNCLASSIFIED//~~FOUO~~

AD Kelly -

I have a short paper and some materials prepared regarding Sen Grassley's letter regarding Insider Threat as it relates to whistleblowers. Is there a specific person in OCA through which I should coordinate?

Thanks,

UC [redacted]
CD-4D

b6
b7C

[redacted]

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

[Redacted] (DO) (FBI)

From: BEERS, ELIZABETH RAE (OCA) (FBI)
Sent: Monday, March 24, 2014 10:53 AM
To: [Redacted] (DO)(FBI); [Redacted] (DO) (FBI); [Redacted] (DO)
(FBI); [Redacted] (DO)(FBI)
Cc: KELLY, STEPHEN (DO)(FBI); [Redacted] (DO) (FBI); [Redacted]
(OCA) (FBI); [Redacted] (DO) (FBI)
Subject: Calendar Items / IMS entries --- UNCLASSIFIED
SentinelCaseId: TRANSITORY RECORD

b6
b7C

Classification: UNCLASSIFIED

=====
TRANSITORY RECORD

[Redacted]

b5
b6
b7C

[Redacted]

UCs - [Redacted]

Thanks,

=====
Classification: UNCLASSIFIED

[redacted] (DO) (FBI)

From: [redacted] (DO) (FBI)
Sent: Monday, March 24, 2014 11:01 AM
To: BEERS, ELIZABETH RAE (OCA) (FBI); [redacted] (DO)(FBI); [redacted] (DO) (FBI); [redacted] (DO) (FBI); [redacted] (DO)(FBI)
Cc: KELLY, STEPHEN (DO)(FBI); [redacted] (DO) (FBI); [redacted] (OCA) (FBI)
Subject: RE: Calendar Items / IMS entries --- UNCLASSIFIED
SentinelCaseId: TRANSITORY RECORD

b6
b7C

Classification: UNCLASSIFIED

Beth,
Apologies for any confusion in our conversation earlier today.
[redacted] was in an internal backbrief from the Insider Threat team for CLU 1.
This was not on the Hill, it was internal FBI and informational.

b6
b7C

v/r,
[redacted]

From: BEERS, ELIZABETH RAE (OCA) (FBI)
Sent: Monday, March 24, 2014 10:53 AM
To: [redacted] (DO)(FBI); [redacted] (DO) (FBI); [redacted] (DO) (FBI); [redacted] (DO)(FBI)
Cc: KELLY, STEPHEN (DO)(FBI); [redacted] (DO) (FBI); [redacted] (OCA) (FBI); [redacted] (DO) (FBI)
Subject: Calendar Items / IMS entries --- UNCLASSIFIED

b6
b7C

Classification: UNCLASSIFIED

TRANSITORY RECORD

[redacted]

b5
b6
b7C

[redacted]

[redacted]

Thanks,

[Redacted] (DO) (FBI)

From: [Redacted] (DO) (FBI)
Sent: Friday, March 28, 2014 4:16 PM
To: KELLY, STEPHEN (DO)(FBI); BEERS, ELIZABETH RAE (OCA) (FBI); [Redacted] (DO)(FBI); [Redacted] (OCA) (FBI); [Redacted] (DO) (FBI); [Redacted] (A) (FBI); [Redacted] (OCA) (FBI); [Redacted] (DO)(FBI); [Redacted] (DO)(FBI); [Redacted] (DO)(FBI); [Redacted] (OCA) (FBI); [Redacted] (DO) (FBI); [Redacted] (DO) (FBI); [Redacted] (DO) (FBI); [Redacted] (DO) (FBI)

b6
b7C

Subject: Calendar items --- UNCLASSIFIED

SentinelCaseId: TRANSITORY RECORD

Classification: UNCLASSIFIED

=====
TRANSITORY RECORD

Calendar items:

Date and Time: April 4, 2014 at 2:00 pm
Event: Briefing
Committee/Staff: Sen. Grassley staff
Location: Hart 135
Topic: *National Insider Threat Program*
FBI Participants: [Redacted] UC, Counterintelligence Division 4D (Insider Threat Investigation)
Other participants: None
Classification: Unclassified
OCA Contact: [Redacted]
OLA Contact: [Redacted]

b6
b7C

Date and Time: April 8, 2014 at 2:30 pm
Event: Hearing
Committee/Staff: Senate Judiciary
Location: Dirksen 226
Topic: *The Problem of Trade Secret Theft*
FBI Participants: Acting Assistant Director Louis Bladel, Counterespionage Section, Counterintelligence Division
Other participants: TBD
Classification: Unclassified
OCA Contact: [Redacted]
OLA Contact: [Redacted]

b6
b7C

=====
Classification: UNCLASSIFIED

[Redacted]

From: [Redacted]
Sent: Monday, April 28, 2014 4:59 PM
To: [Redacted]
Subject: RE: Insider Threat presentation slide deck

b6
b7C

It should be treated as ~~FOUO~~, but otherwise there is no problem in sharing.

Thanks,

UC [Redacted]
Counterespionage Section, FBIHQ
Co-Director, National Insider Threat Task Force

b6
b7C

[Redacted]

From: [Redacted]
Sent: Monday, April 28, 2014 2:26 PM
To: [Redacted]
Subject: Insider Threat presentation slide deck

b6
b7C

Hi [Redacted]

[Redacted]

b5

[Redacted], ~~FOUO~~,

Thanks as always,

[Redacted]

[Redacted]

b6
b7C

From: Kelly, Stephen
Sent: Monday, April 14, 2014 4:30 PM
To: Kelly, Stephen [Redacted] (Judiciary-Rep) [Redacted] (Judiciary-Rep)
Cc: [Redacted]
Subject: RE: Information Assurance Training - Insider Threat

[Redacted]

b5

[Redacted]

Thanks.

- Stephen

Stephen D. Kelly
Assistant Director
Office of Congressional Affairs
Federal Bureau of Investigation

[Redacted]

b6
b7C

From: Kelly, Stephen
Sent: Monday, April 14, 2014 4:15 PM
To: [Redacted] (Judiciary-Rep) [Redacted] (Judiciary-Rep)
Cc: [Redacted]
Subject: Information Assurance Training - Insider Threat

b6
b7C

[Redacted]

As we discussed, it appears that the information assurance training that the FBI requires for all employees includes a "insider threat" section, along with numerous other sections. It's my understanding that this training is developed by the Defense Information Security Agency and is available for you to review online at this link: <http://iase.disa.mil/eta/cyberchallenge/launchPage.htm>. As you can see at this link, this training has three versions for DoD, Federal Agencies, and the Intelligence Community. I believe we use the federal agencies version, but I will confirm that for you. As I mentioned to you, I apologize in advance because the format of the training is not particularly user friendly for your purposes. You need to launch the program and then go through a step-by-step process to get to the section on insider threat, which is a relatively small part of the overall training. This is the format that we have internally, so we're not immediately able to provide it to you in another format. Also, as I mentioned, I have gone through the insider threat piece, which includes several case examples and a series of exercises designed to identify possible insider threat vulnerabilities, but I do not believe there is any mention of whistleblowers or their protections. That being said, I wanted you to see it for yourself, and let me know if you have trouble accessing this link.

We will look further to see if there are other materials that may be responsive to your request, but I wanted to send this along now as this training is provided to all employees, as well as the earlier DVDs that were provided earlier.

- Stephen

Stephen D. Kelly
Assistant Director
Office of Congressional Affairs
Federal Bureau of Investigation

[Redacted]

b6
b7C

From: [Redacted] (Judiciary-Rep)
Sent: Wednesday, April 16, 2014 11:56 AM
To: Kelly, Stephen [Redacted] (Judiciary-Rep)
Cc: [Redacted] (Judiciary-Dem)
Subject: RE: Information Assurance Training - Insider Threat

Correction: It looks like we were able to access it on a second attempt.

From: [Redacted] (Judiciary-Rep)
Sent: Wednesday, April 16, 2014 10:59 AM
To: 'Kelly, Stephen' [Redacted] (Judiciary-Rep)
Cc: [Redacted] (Judiciary-Dem)
Subject: RE: Information Assurance Training - Insider Threat

b6
b7C

We cannot access the intelligence community version from the link you provided. It looks like you'll need to figure out another way to get the relevant portion to us.

From: Kelly, Stephen [mailto:[Redacted]]
Sent: Monday, April 14, 2014 4:30 PM
To: Kelly, Stephen [Redacted] (Judiciary-Rep); [Redacted] (Judiciary-Rep)
Cc: [Redacted] (Judiciary-Dem)
Subject: RE: Information Assurance Training - Insider Threat

b6
b7C

One correction. It appears that we use the Intelligence Community version of this information assurance training, which includes sections on SCI procedures and working in SCIFs, which are not in the Federal Agencies version. This is the third option on the link attached to the prior e-mail.

Thanks.

- Stephen

Stephen D. Kelly
Assistant Director
Office of Congressional Affairs
Federal Bureau of Investigation

[Redacted]

b6
b7C

From: Kelly, Stephen
Sent: Monday, April 14, 2014 4:15 PM
To: [Redacted] (Judiciary-Rep); [Redacted] (Judiciary-Rep)
Cc: [Redacted]
Subject: Information Assurance Training - Insider Threat

[Redacted]


b6
b7C

As we discussed, it appears that the information assurance training that the FBI requires for all employees includes a "insider threat" section, along with numerous other sections. It's my understanding that this training is developed by the Defense Information Security Agency and is available for you to review online at this link: <http://iase.disa.mil/eta/cyberchallenge/launchPage.htm>. As you can see at this link, this training has three versions for DoD, Federal Agencies, and the Intelligence Community. I believe we use the federal agencies version, but I will confirm

that for you. As I mentioned to you, I apologize in advance because the format of the training is not particularly user friendly for your purposes. You need to launch the program and then go through a step-by-step process to get to the section on insider threat, which is a relatively small part of the overall training. This is the format that we have internally, so we're not immediately able to provide it to you in another format. Also, as I mentioned, I have gone through the insider threat piece, which includes several case examples and a series of exercises designed to identify possible insider threat vulnerabilities, but I do not believe there is any mention of whistleblowers or their protections. That being said, I wanted you to see it for yourself, and let me know if you have trouble accessing this link.

We will look further to see if there are other materials that may be responsive to your request, but I wanted to send this along now as this training is provided to all employees, as well as the earlier DVDs that were provided earlier.

- Stephen

Stephen D. Kelly
Assistant Director
Office of Congressional Affairs
Federal Bureau of Investigation


b6
b7C

[Redacted]

b6
b7C

From: [Redacted]
Sent: Thursday, January 30, 2014 12:35 PM
To: [Redacted] (Judiciary-Rep)
Subject: RE: Letter re Insider threat videos

[Redacted]

I should have a better picture by this afternoon or tomorrow morning, will follow up with you on any details,
Thanks

b6
b7C

[Redacted]

From: [Redacted] (Judiciary-Rep) [mailto:[Redacted]]
Sent: Wednesday, January 29, 2014 3:49 PM
To: [Redacted]
Subject: RE: Letter re Insider threat videos

[Redacted]

Have you been able to find an answer to this question?

b6
b7C

Thank you.

[Redacted]

[Redacted]

Investigative Counsel
Ranking Member Charles E. Grassley
U.S. Senate Committee on the Judiciary

[Redacted]

From: [Redacted] (Judiciary-Rep)
Sent: Thursday, January 09, 2014 2:39 PM
To: [Redacted]
Subject: RE: Letter re Insider threat videos

[Redacted]

Thank you for the very prompt response to Senator Grassley's letter. I just got back in the office yesterday after being out on paternity leave, and received the videos then. However, I did want to just check—does this mean that there are no other training materials regarding the National Insider Threat Program or any FBI-specific insider threat program?

b6
b7C

Thanks,

[Redacted]

[Redacted]

Investigative Counsel
Ranking Member Charles E. Grassley
U.S. Senate Committee on the Judiciary

[Redacted]

From [redacted] [mailto:[redacted]]
Sent: Tuesday, December 31, 2013 2:29 PM
To [redacted] Judiciary-Rep); CEG (Judiciary-Rep)
Subject: Letter re Insider threat videos

b6
b7C

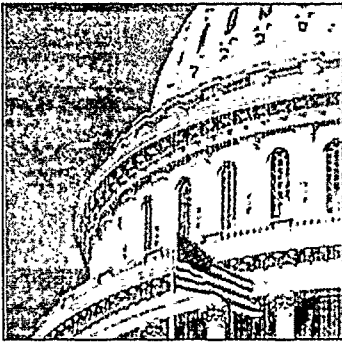
Letter from FBI, response to Sen. Grassley's of Dec. 17, 2013, requesting copy of videos re: insider threat. Hard copies of letter and videos were also hand-delivered to SJC Minority office, Dirksen 152 on December 31, 2013.

A company can often detect or control when an outsider (non-employee) tries to access company data either physically or electronically, and can mitigate the threat of an outsider stealing company property. However, the thief who is harder to detect and who could cause the most damage is the insider—the employee with legitimate access. That insider may steal solely for personal gain, or that insider may be a “spy”—someone who is stealing company information or products in order to benefit another organization or country.

The Insider Threat
An introduction to detecting and deterring an insider spy.
[View printable version \(pdf\)](#)

This brochure serves as an introduction for managers and security personnel on how to detect an insider threat and provides tips on how to safeguard your company's trade secrets.

Protect Your Intellectual Property



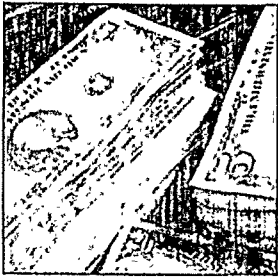
Theft of intellectual property is an increasing threat to organizations, and can go unnoticed for months or even years.

There are increased incidents of employees taking proprietary information when they believe they will be, or are, searching for a new job.

Congress has continually expanded and strengthened criminal laws for violations of intellectual property rights to protect innovation and ensure that egregious or persistent intellectual property violations do not merely become a standard cost of doing business.

A domestic or foreign business competitor or foreign government intent on illegally acquiring a company's proprietary information and trade secrets may wish to place a spy into a company in order to gain access to non-public information. Alternatively, they may try to recruit an existing employee to do the same thing.

Personal Factors



There are a variety of motives or personal situations that may increase the likelihood someone will spy against their employer:

Greed or Financial Need: A belief that money can fix anything. Excessive debt or overwhelming expenses.

Anger/Revenge: Disgruntlement to the point of wanting to retaliate against the organization.

Problems at work: Lack of recognition, disagreements with co-workers or managers, dissatisfaction with the job, a pending layoff.

Ideology/Identification: A desire to help the "underdog" or a particular cause.

Divided Loyalty: Allegiance to another person or company, or to a country besides the United States.

Adventure/Thrill: Want to add excitement to their life, intrigued by the clandestine activity, "James Bond Wannabe."

Vulnerability to blackmail: Extra-marital affairs, gambling, fraud.

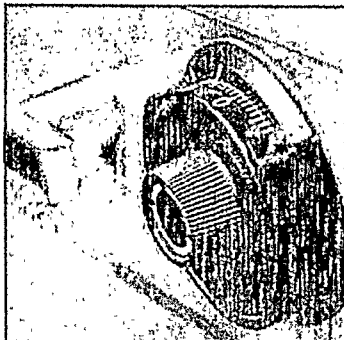
Ego/Self-image: An "above the rules" attitude, or desire to repair wounds to their self-esteem. Vulnerability to flattery or the promise of a better job. Often coupled with Anger/Revenge or Adventure/Thrill.

Ingratiation: A desire to please or win the approval of someone who could benefit from insider information with the expectation of returned favors.

Compulsive and destructive behavior: Drug or alcohol abuse, or other addictive behaviors.

Family problems: Marital conflicts or separation from loved ones.

Organizational Factors



Organizational situations may increase the ease for thievery:

The availability and ease of acquiring proprietary, classified, or other protected materials. Providing access privileges to those who do not need it.

Proprietary or classified information is not labeled as such, or is incorrectly labeled.

The ease that someone may exit the facility (or network system) with proprietary, classified or other protected materials.

Undefined policies regarding working from home on projects of a sensitive or proprietary nature.



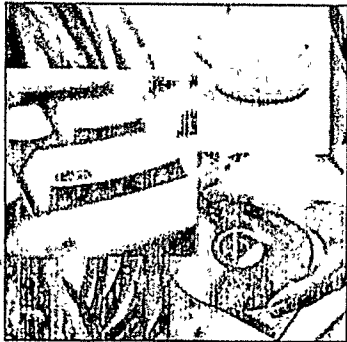
The perception that security is lax and the consequences for theft are minimal or non-existent.

Time pressure: Employees who are rushed may inadequately secure proprietary or protected materials, or not fully consider the consequences of their actions.

Employees are uncertain on how to properly protect proprietary information.

Behavioral Indicators

Some behaviors may be a clue that an employee is spying and/or methodically stealing from the organization:



Without need or authorization, takes proprietary or other material home via documents, thumb drives, computer disks, or e-mail. Inappropriately seeks or obtains proprietary or classified information on subjects not related to their work duties.

Interest in matters outside the scope of their duties, particularly those of interest to foreign entities or business competitors.

Unnecessarily copies material, especially if it is proprietary or classified.

Remotely accesses the computer network while on vacation, sick leave, or at other odd times.

Disregards company computer policies on installing personal software or hardware, accessing restricted websites, conducting unauthorized searches, or downloading confidential information.

Works odd hours without authorization; notable enthusiasm for overtime work, weekend work, or unusual schedules when clandestine activities could be more easily conducted.

Unreported foreign contacts (particularly with foreign government officials or intelligence officials) or unreported overseas travel.



Short trips to foreign countries for unexplained or strange reasons.

Unexplained affluence; buys things that they cannot afford on their household income.

Engages in suspicious personal contacts, such as with competitors, business partners or other unauthorized individuals.

Covered by life crises or career disappointments.

Shows unusual interest in the personal lives of co-workers; asks inappropriate questions regarding finances or relationships.

Concern that they are being investigated; leave traps to detect searches of their work area or home; searches for listening devices or cameras.

Many people experience or exhibit some or all of the above to varying degrees; however, most people will not cross the line and commit a crime.

You Can Make A Difference

Organizations need to do their part to deter intellectual property theft:

- Educate and regularly train employees on security or other protocols.
- Ensure that proprietary information is adequately, if not robustly, protected.
- Use appropriate screening processes to select new employees.
- Provide non-threatening, convenient ways for employees to report suspicions.
- Routinely monitor computer networks for suspicious activity.
- Ensure security (to include computer network security) personnel have the tools they need.

Remind employees that reporting security concerns is vital to protecting your company's intellectual property, its reputation, its financial well-being, and its future. They are protecting their own jobs. Remind them that if they see something, to say something.

Get Assistance

Being aware of potential issues, exercising good judgment, and conducting discrete inquiries will help you ascertain if there is a spy in your midst. However, if you believe one of your employees is a spy or is stealing company trade secrets, do not alert the person to the fact that he/she is under suspicion, but seek assistance from trained counterintelligence experts—such as the FBI. The FBI has the tools and experience to identify and mitigate such threats. If asked to investigate, the FBI will minimize the disruption to your business, and safeguard your privacy and your data. Where necessary, the FBI will seek protective orders to preserve trade secrets and business confidentiality. The FBI is committed to maintaining the confidentiality and competitive position of US companies. The FBI will also provide security and counterintelligence training or awareness seminars for you and your employees upon request.

Recent Insider Theft Cases

Wen Chyu Liu, a retired research scientist, was sentenced in January 2012 to 60 months in prison, two years supervised release, a \$25,000 fine and was ordered to forfeit \$600,000. Liu was convicted in February 2011 of stealing trade secrets from his former employer and selling them to companies in China. Liu conspired with at least four current and former employees, traveled throughout China to market the stolen information, paid current and former employees for material and information, and bribed a then-employee with \$50,000 in cash to provide a process manual and other information.

Kexue Huang was employed by two different US companies. He admitted that from 2007 to 2010 he delivered stolen trade secrets from both companies to individuals in Germany and China. The stolen materials were used to conduct unauthorized research to benefit Chinese universities. Huang also pursued steps to develop and produce the trade secrets in China. The aggregated loss from both companies was between \$7 and \$20 million. Huang pleaded guilty to charges of economic espionage and theft of trade secrets, and was sentenced in December 2011 to 87 months in prison and three years supervised release.

Yuan Li, a former research chemist with a global pharmaceutical company, pleaded guilty in January 2012 to stealing her employer's trade secrets and making them available for sale through Abby Pharmatech, Inc. Li was a 50% partner in Abby. Between October 2008 and June 2011 Li accessed her employer's internal databases, downloaded information to her personal home computer, and made them for sale through Abby. She was sentenced to 18 months in prison.

Elliot Doxer sent an e-mail to the Israeli Consulate stating that he was willing to provide information from his employer that might help Israel. An undercover FBI agent posing as an Israeli intelligence officer spoke to Doxer and established a "dead drop" where the two could exchange information. For the next 18 months, Doxer visited the dead drop at least 62 times. Doxer provided customer and employee lists, contract information, and other trade secrets. He pleaded guilty to one count of foreign economic espionage and was sentenced in December 2011 to six months in prison, six months home confinement, and fined \$25,000.

Sergey Aleynikov worked as a computer programmer for a Wall Street company. During his last few days at that company, he transferred 32 megabytes of proprietary computer codes — a theft that could have cost his employer millions of dollars. He attempted to hide his activities but the company discovered irregularities through its routine network monitoring systems. In December 2010, Aleynikov was found guilty of theft of trade secrets.

Michael Mitchell became disgruntled and was fired from his job due to poor performance. He kept numerous computer files with his employer's trade secrets; he entered into a consulting agreement with a rival Korean company and gave them the stolen trade secrets. In March 2010, he was sentenced to 18 months in prison and ordered to pay his former employer over \$187,000.

Shalin Jhaveri gave trade secrets to a person he believed was an investor willing to finance a business venture in India, and confirmed that the information he had taken from his employer was everything he needed to start the business. In January 2011, he was sentenced to time served (one year and fifteen days), three years probation, a \$5,000 fine, and a \$100 Special Assessment.

Lanjuan Jin took a leave of absence from her US employer in 2006. While on leave, Jin worked for a similar company in China. A year later, Jin returned to the United States. Within a week of her return, she bought a one-way ticket back to China, and advised her US employer that she was ready to end her leave. Jin returned to work on February 26, 2007 and for the next two days downloaded hundreds of technical documents. On February 28, 2007, during a routine check at the airport, more than 1,000 electronic and paper documents proprietary to her US employer were found in Jin's luggage. In 2012, Jin was sentenced to four years in prison and fined \$20,000.

Greg Chung spied for China from 1979-2006. Chung stole trade secrets about the space shuttle, the Delta IV rocket and the C-17 military cargo jet for the benefit of the Chinese government. Chung's motive was to "contribute to the Motherland." He stole hundreds of thousands of documents from his employer. He traveled to China under the guise of giving lectures while secretly meeting with Chinese agents. He also used Mak (below) to transfer information back to China. In February 2010 he was sentenced to over 15 years in prison.

Chi Mak admitted that he was sent to the United States in 1978 in order to obtain employment in the defense industry with the goal of stealing US defense secrets, which he did for over 20 years. He passed information on quiet electric propulsion systems for US submarines, details on the Aegis radar system, and information on stealth ships being developed by the US Navy. The Chinese government tasked Mak to acquire information on other technologies. Mak recruited family members to encrypt and covertly courier information back to China. In May 2007, Mak was convicted of conspiracy, failing to register as an agent of a foreign government, and other violations. He was sentenced to over 24 years in prison.

Report theft of trade secrets to your local FBI office or submit a tip online: tips.fbi.gov



Congressional Affairs Office Congressional Contacts

Event Date: 3/12/2014 Classification Level: UnClassified

Date Entered: 03/12/2014 2014-600 Proactive Reactive

Briefing Hearing SAC CV HQ CV FOC Other # of SAC CV Visits: 0

Brief Type: Event Date: 3/12/2014 Event Time:

Entered By: [Redacted] Unit: CLU II

Topic: Acknowledgement from Grassley staffer [Redacted] that he did not respond to FBI's offer more than a month ago for a briefing on the matter of Insider Threat program, and request for a briefing. Division: [Redacted]

b6
b7C

OCA Contact Person: [Redacted]

DOJ Contact: [Redacted] Date: [Redacted] Attended: [Redacted]

FBI Participants: [Redacted]

Other Participants:

Committees
/Subcommittees

Members/Staff: [Redacted] Grassley staffer

b6
b7C

Executive Summary:

[Redacted] re Insider Threat program briefing

Details of Event:

Acknowledgement from Grassley staffer [Redacted] that he did not respond to FBI's offer more than a month ago for a briefing on the matter of Insider Threat program. Agent [Redacted] renewed the offer of a briefing. [Redacted] agreed. Will follow up with prospective date/time.

b6
b7C

Follow Up Action:

Attachment:

0

[Redacted]

From: [Redacted]
Sent: Friday, February 07, 2014 3:38 PM
To: [Redacted] (Judiciary-Rep)
Subject: RE: Letter re Insider threat videos

b6
b7C

[Redacted] following up on a short voicemail I left a moment ago – it looks like a briefing may best answer your questions on the subject, so perhaps we could coordinate something for the week of the 24th; let me know how that works and we'll see what we can line up

Thanks,

[Redacted]

From: [Redacted] (Judiciary-Rep) [mailto:[Redacted]]
Sent: Thursday, February 06, 2014 11:06 AM
To: [Redacted]
Subject: RE: Letter re Insider threat videos

b6
b7C

[Redacted]

What were you able to learn? I never heard back from you last week.

Thanks,

[Redacted]

From: [Redacted] [mailto:[Redacted]]
Sent: Thursday, January 30, 2014 12:35 PM
To: [Redacted] (Judiciary-Rep)
Subject: RE: Letter re Insider threat videos

b6
b7C

Hi [Redacted]

I should have a better picture by this afternoon or tomorrow morning, will follow up with you on any details,

Thanks

[Redacted]

From: [Redacted] (Judiciary-Rep) [mailto:[Redacted]]
Sent: Wednesday, January 29, 2014 3:49 PM
To: [Redacted]
Subject: RE: Letter re Insider threat videos

[Redacted]

Have you been able to find an answer to this question?

b6
b7C

Thank you,

[Redacted]

[Redacted]

Investigative Counsel

Ranking Member Charles E. Grassley
U.S. Senate Committee on the Judiciary

[Redacted]

b6
b7C

From: [Redacted] (Judiciary-Rep)
Sent: Thursday, January 09, 2014 2:39 PM
To: [Redacted]
Subject: RE: Letter re Insider threat videos

[Redacted]

Thank you for the very prompt response to Senator Grassley's letter. I just got back in the office yesterday after being out on paternity leave, and received the videos then. However, I did want to just check—does this mean that there are no other training materials regarding the National Insider Threat Program or any FBI-specific insider threat program?

Thanks,

[Redacted]

[Redacted]

Investigative Counsel
Ranking Member Charles E. Grassley
U.S. Senate Committee on the Judiciary

[Redacted]

b6
b7C

From: [Redacted] [mailto:[Redacted]]
Sent: Tuesday, December 31, 2013 2:29 PM
To: [Redacted] (Judiciary-Rep); CEG (Judiciary-Rep)
Subject: Letter re Insider threat videos

Letter from FBI, response to Sen. Grassley's of Dec. 17, 2013, requesting copy of videos re: insider threat. Hard copies of letter and videos were also hand-delivered to SJC Minority office, Dirksen 152 on December 31, 2013.

[Redacted]

From: [Redacted] (Judiciary-Rep) [Redacted]
Sent: Wednesday, March 12, 2014 3:54 PM
To: [Redacted]
Subject: RE: Letter re Insider threat videos

b6
b7C

[Redacted]

Thanks for looking into updated briefing dates, and I apologize I never got back to you on this before. Again, to reiterate Senator Grassley's request, if there are any additional training materials on the Insider Threat Program, whether intended FBI-specific or intended for the training of other agencies through the National Insider Threat Program, we would like those to be produced to the Committee (both majority and minority). If the briefer would like to walk us through such materials, that would be great, but any briefing would be most helpful in the context of the materials themselves.

Best,

[Redacted]

[Redacted]

Investigative Counsel
Ranking Member Charles E. Grassley
U.S. Senate Committee on the Judiciary

[Redacted]

b6
b7C

From: [Redacted] [mailto:[Redacted]]
Sent: Friday, February 07, 2014 3:38 PM
To: [Redacted] (Judiciary-Rep)
Subject: RE: Letter re Insider threat videos

b6
b7C

[Redacted] following up on a short voicemail I left a moment ago – it looks like a briefing may best answer your questions on the subject, so perhaps we could coordinate something for the week of the 24th; let me know how that works and we'll see what we can line up

Thanks,

[Redacted]

From: [Redacted] (Judiciary-Rep) [mailto:[Redacted]]
Sent: Thursday, February 06, 2014 11:06 AM
To: [Redacted]
Subject: RE: Letter re Insider threat videos

[Redacted]

What were you able to learn? I never heard back from you last week.

b6
b7C

Thanks,

[Redacted]

From: [Redacted] [mailto:[Redacted]]
Sent: Thursday, January 30, 2014 12:35 PM

To: [redacted] (Judiciary-Rep)
Subject: RE: Letter re Insider threat videos

b6
b7C

H [redacted]
I should have a better picture by this afternoon or tomorrow morning, will follow up with you on any details,
Thanks

[redacted]

From: [redacted] (Judiciary-Rep) [mailto:[redacted]]
Sent: Wednesday, January 29, 2014 3:49 PM
To: [redacted]
Subject: RE: Letter re Insider threat videos

[redacted]

b6
b7C

Have you been able to find an answer to this question?

Thank you,

[redacted]

[redacted]

Investigative Counsel
Ranking Member Charles E. Grassley
U.S. Senate Committee on the Judiciary

[redacted]

From: [redacted] (Judiciary-Rep)
Sent: Thursday, January 09, 2014 2:39 PM
To: [redacted]
Subject: RE: Letter re Insider threat videos

[redacted]

Thank you for the very prompt response to Senator Grassley's letter. I just got back in the office yesterday after being out on paternity leave, and received the videos then. However, I did want to just check—does this mean that there are no other training materials regarding the National Insider Threat Program or any FBI-specific insider threat program?

b6
b7C

I thank.

[redacted]

[redacted]

Investigative Counsel
Ranking Member Charles E. Grassley
U.S. Senate Committee on the Judiciary

[redacted]

From: [redacted] [mailto:[redacted]]
Sent: Tuesday, December 31, 2013 2:29 PM
To: [redacted] (Judiciary-Rep); CEG (Judiciary-Rep)
Subject: Letter re Insider threat videos

b6
b7C

Letter from FBI, response to Sen. Grassley's of Dec. 17, 2013, requesting copy of videos re: insider threat. Hard copies of letter and videos were also hand-delivered to SJC Minority office, Dirksen 152 on December 31, 2013.

United States Senate

December 17, 2013

VIA ELECTRONIC TRANSMISSION

The Honorable James B. Comey, Jr.
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, DC 20535

Dear Director Comey:

On October 28, 2013, I received a letter from the Federal Bureau of Investigation (FBI) in which it indicated that it had collaborated with the Office of the Director of National Intelligence (ODNI) on two training videos about the FBI's National Insider Threat Program. The videos, titled *Betrayed* and *Game of Pawns*, were developed jointly by the FBI's Counterintelligence Division and ODNI's Office of the National Counterintelligence Executive (ONCIX). The FBI has also produced other insider threat materials, such as the brochure, *The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy*.¹

As I understand it, the National Insider Threat Program is the result of Executive Order 13587, issued by President Obama in October 2011, which established an interagency Insider Threat Task Force, to be staffed by the FBI and the ONCIX.² It also directed Executive Branch departments and agencies to develop their own insider threat programs. The President subsequently issued a Presidential Memorandum in November 2012 transmitting the National Insider Threat Policy and setting forth minimum standards for departmental and agency programs.³

These efforts have subsequently received press attention, some of which has focused on concerns about whether the program adequately protects whistleblowers.⁴

¹ Federal Bureau of Investigation, *The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy*, http://www.fbi.gov/about-us/investigate/counterintelligence/insider_threat_brochure.

² Executive Order 13587 – Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011. Available at <http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-structural-reforms-improve-security-classified-networks->.

³ Presidential Memorandum – National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Nov. 21, 2012. Available at <http://www.whitehouse.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand>.

⁴ For example, Marisa Taylor and Jonathan S. Landay, "Obama's crackdown views leaks as aiding enemies of U.S.," *McClatchy* (Jun. 20, 2013), available at

As you know, I strongly believe that whistleblowers play an important role in safeguarding the federal government against waste, fraud, and abuse. You too stated in your confirmation hearing that you believe whistleblowers are a critical element of a functioning democracy. Their willingness to come forward contributes to improving government operations. They often put themselves at risk of reprisal from their employers, sometimes being demoted, reassigned, or fired as a result of their actions. Under the Whistleblower Protection Act and Presidential Policy Directive 19, federal employees may not be retaliated against for reporting waste, fraud, and abuse.⁵

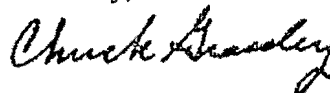
Accordingly, some agencies have taken steps to prevent the insider threat program from chilling whistleblower communications. For example, the Office of the Inspector General for the Intelligence Community is developing training that integrates whistleblowing into the agency processes, making the Intelligence Community whistleblowing and insider threat programs mutually reinforcing.

In order to assess whether training materials on the National Insider Threat Program provide adequate guidance on protecting whistleblowers, I respectfully request that you provide me with copies of *Betrayed* and *Game of Pawns*, as well as copies of any other training materials regarding the National Insider Threat Program or any FBI-specific insider threat program. I would appreciate receiving these materials by January 14, 2014. I know that you consider transparency to be an important value, and I trust that transparency on this issue will benefit both whistleblowers and our national security.

Should you have any questions regarding this letter, please contact [redacted] [redacted] of my staff at [redacted]

b6
b7C

Sincerely,



Charles E. Grassley
Ranking Member

cc: The Honorable James R. Clapper
Director of National Intelligence

[Redacted]

From: [Redacted] (Judiciary-Rep)
Sent: Thursday, January 09, 2014 2:39 PM
To: [Redacted]
Subject: RE: Letter re Insider threat videos

b6
b7C

[Redacted]

Thank you for the very prompt response to Senator Grassley's letter. I just got back in the office yesterday after being out on paternity leave, and received the videos then. However, I did want to just check—does this mean that there are no other training materials regarding the National Insider Threat Program or any FBI-specific insider threat program?

Thanks,

[Redacted]

[Redacted]
Investigative Counsel
Ranking Member Charles E. Grassley
U.S. Senate Committee on the Judiciary

b6
b7C

From: [Redacted] [mailto:[Redacted]]
Sent: Tuesday, December 31, 2013 2:29 PM
To: [Redacted] (Judiciary-Rep); CEG (Judiciary-Rep)
Subject: Letter re Insider threat videos

Letter from FBI, response to Sen. Grassley's of Dec. 17, 2013, requesting copy of videos re: insider threat. Hard copies of letter and videos were also hand-delivered to SJC Minority office, Dirksen 152 on December 31, 2013.



Congressional Affairs Office Congressional Contacts

Event Date: 1/30/2014 Classification Level: Unclassified

Date Entered: 01/30/2014 2014-522 Proactive Reactive

Briefing Hearing SAC CV HQ CV FOC Other # of SAC CV Visits: 0

Brief Type: Event Date: 1/30/2014 Event Time:

Entered By: [Redacted] Unit: CLU II

Topic: Sen. Grassley staffer [Redacted] inquiry re status of any additional Insider Threat training details. Division: [Redacted]

OCA Contact Person: [Redacted]

DOJ Contact: [Redacted] Date: [Redacted] Attended: [Redacted]

FBI Participants: [Redacted]

Other Participants:

Committees
/Subcommittees

Members/Staff: Sen. Grassley staffer [Redacted]

Executive Summary:

Sen. Grassley staffer [Redacted] inquiry re status of any additional Insider Threat training details.

Details of Event:

Sen. Grassley staffer [Redacted] inquiry re status of any additional Insider Threat training details. Advised staffer that additional details may be available, will get back when/if any available.

Follow Up Action:

Attachment:

0

b6
b7C

b6
b7C



Congressional Affairs Office Congressional Contacts

Event Date: 2/7/2014 Classification Level: UnClassified

Date Entered: 02/07/2014 2014-552 Proactive Reactive

Briefing Hearing SAC CV HQ CV FOC Other # of SAC CV Visits: 0

Brief Type: Event Date: 2/7/2014 Event Time:

Entered By: [Redacted] Unit: CLU II

Topic: Steps to coordinate briefing for Sen. Grassley staffer [Redacted] re Insider Threat program training Division: [Redacted]

b6
b7C

OCA Contact Person: [Redacted]

DOJ Contact: [Redacted] Date: [Redacted] Attended: [Redacted]

FBI Participants: [Redacted]

Other Participants:

Committees
/Subcommittees

Members/Staff: [Redacted] staffer for Sen. Grassley (IA)

Executive Summary:

Steps to coordinate briefing for Sen. Grassley staffer [Redacted] re Insider Threat program training

b6
b7C

Details of Event:

Steps to coordinate briefing for Sen. Grassley staffer [Redacted] re Insider Threat program training. Questions that staffer has do not lend themselves to yes or no answers, so briefing in the format of a Q&A is proposed to staffer through the CD-4D unit.

Follow Up Action:

Attachment:

0



Congressional Affairs Office Congressional Contacts

Event Date: 4/16/2014

Classification Level: UnClassified

Date Entered: 04/16/2014

2014-627

Proactive Reactive

Briefing Hearing SAC CV HQ CV FOC Other # of SAC CV Visits: 0

Brief Type: Event Date: 4/16/2014 Event Time:

Entered By: [Redacted]

Unit: CLU II

Topic: Grassley staffer [Redacted] re insider threat video training access link sent by AD Kelly Division: [Redacted]

OCA Contact Person: [Redacted]

DOJ Contact: [Redacted] Date: [Redacted] Attended: [Redacted]

FBI Participants: [Redacted]

Other Participants:

Committees /Subcommittees

Members/Staff: [Redacted] Grassley staffer

Executive Summary:

Grassley staffer [Redacted] re insider threat video training access link sent by AD Kelly.

Details of Event:

Grassley staffer [Redacted] re Defense Information Security Agency insider threat video training access link sent by AD Kelly [Redacted] claimed unable to access, then later acknowledged ability to access link on computer.

Follow Up Action:

Attachment:

0

b6
b7C

b6
b7C

b6
b7C