ENHANCING YOUR INTELLIGENCE AGENCY INFORMATION RESOURCE IQ:

PT. 6 JUSTICE DEPT., FOREIGN INTELLIGENCE SURVEILLANCE COURT, CONGRESSIONAL COMMITTEES, AND CONGRESSIONAL RESEARCH SERVICE

Professor Bert Chapman
Purdue University Libraries
FDLP Academy
February 14, 2019

PURDUE UNIVERSITY
Libraries

Graphic design contributions by Aly Edmondson, Purdue University Libraries

JUSTICE DEPT. INTELLIGENCE RELATED ACTIVITIES

- Federal Bureau of Investigation (FBI)
- Cybercrime.gov
- Foreign Agent Registration Act
- Foreign Intelligence Surveillance Act (FISA) Court
- National Security Division
- Office of Privacy & Civil Liberties

Field Offices | FBI Headquarters | Overseas Offices

Ankara, Turkey

American Embassy: 011-90-312-455-5555
Istanbul Suboffice
American Consulate: 011-90-212-335-9000
Nations covered: Turkey

Counterintelligence missions include:

Protecting the U.S. from terrorist attack

Protecting the U.S. from foreign intelligence operations and espionage

Protecting the U.S. against cyber attacks and high-technology crimes.

Combating transnational and national criminal organizations and enterprises

www.fbi.gov/investigate/counterintelligence

56 U.S. field offices and 63 foreign legal attaches

18 USC 1831 and 18 USC 1832 key governing statutes.

FBI COUNTERINTELLIGENCE

- Counterintelligence responsibilities begin in 1917; nine years after Bureau's 1908 creation.
- Foreign Influence Task Force-Characteristics of foreign influence operations include:
- Targeting U.S. officials and other U.S. individuals through traditional intelligence tradecraft.
- Criminal efforts to suppress voting and illegal campaign financing.
- Cyber attacks against voting infrastructure with computer intrusions targeting elected officials and others.

Protected Voices: Passwords

The FBI's Protected Voices initiative provides cybersecurity recommendations to political campaigns on multiple topics, including passwords, to help mitigate the risk of cyber influence operations targeting U.S. elections.

Video Transcript

Hi, I'm Karen, a special agent with the FBI, and I'd like to share with you some things you can do to prevent attackers from accessing your campaign's networks.

We all use passwords. We use them for our phones, our login to our computers, our email, or other personal online accounts.

Unfortunately, many of us use simple passwords, such as "Password1" or "1234," because they're easier to remember.

Some of us even reuse the same simple password for multiple accounts.

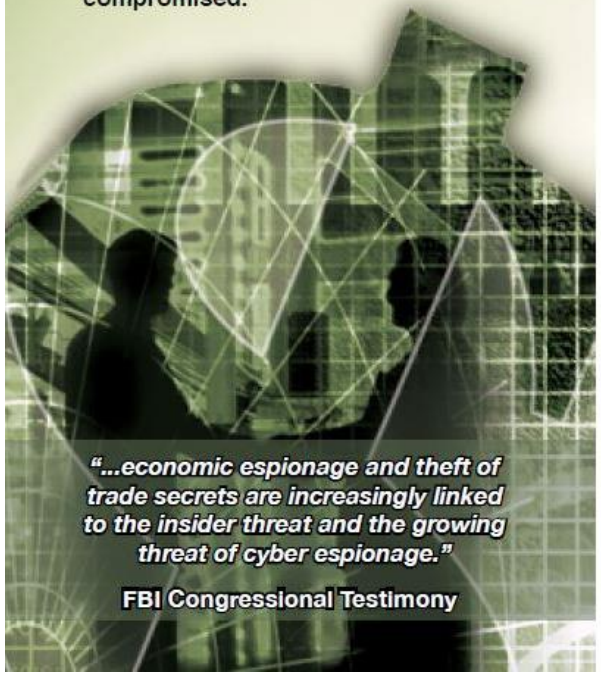
If you use a simple password or pattern of characters, such as "a1b2C#" it's considerably easier for a criminal to crack, which means you've allowed an attacker to access all your accounts linked to that simple password.

It's common that passwords are required to include uppercase letters, lowercase letters, numbers, and special characters. However, recent guidance from the National Institute of Standards and Technology advises that password length is much more beneficial than complexity.

Consider using a passphrase—which is when you combine multiple words into one long string of characters—instead of a password. The extra length of a passphrase makes it harder to crack, such as "WeAreProtectedVoices@2018" or "Ohsaycanyousee" with special characters replacing a few of the letters.

Methods for Economic Protection

1. Recognize the threat.
2. Identify and value trade secrets.
3. Implement a definable plan for safeguarding trade secrets.
4. Secure physical trade secrets and limit access to trade secrets.
5. Provide ongoing security training to employees.
6. Develop an insider threat program.
7. Proactively report suspicious incidents to the FBI before your proprietary information is irreversibly compromised.



"...economic espionage and theft of trade secrets are increasingly linked to the insider threat and the growing threat of cyber espionage."

FBI Congressional Testimony

Commonly Asked Questions

Q Does the 1996 EEA apply if the offender is a foreign person?

A Yes. The Act applies to whoever knowingly performs targeting or acquisition of trade secrets. Territorial limits will apply for prosecution.

Q Does the act help victims of Economic Espionage to protect their trade secrets?

A Yes. The Act contains a special provision to protect the disclosure of trade secret information during the criminal justice process.

Q Are there other statutes that can apply if trade secrets are not protected and therefore cannot be prosecuted under the Act?

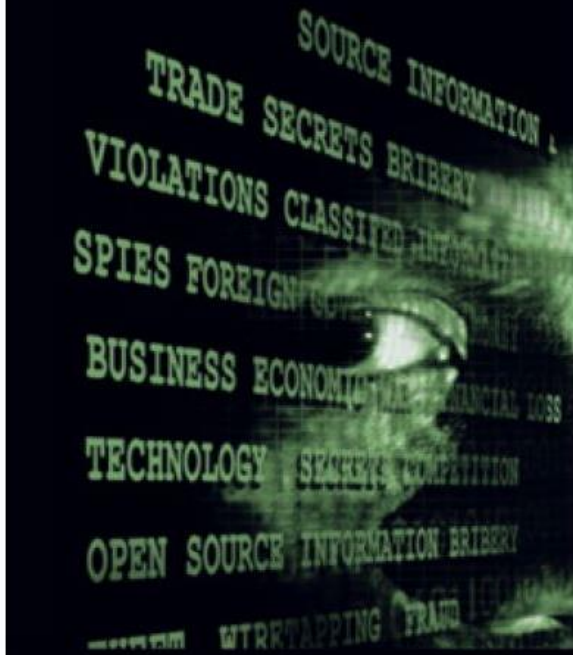
A Yes. The following is a list of violations that may apply: Mail Fraud, Wire Fraud, Computer Fraud and Abuse, Interstate Transportation of Stolen Property, and various Export Control and Intellectual Property Rights statutes. Contact your local FBI field office for further assistance.

Q Is the FBI proactive in its approach to economic espionage?

A Yes. The FBI Director has designated espionage as the FBI's number two priority - second only to terrorism. The Economic Espionage Unit is dedicated to countering the economic espionage threat to include developing training and outreach materials; participating in conferences; visiting private industry; working with the law enforcement and intelligence community on requirement issues; and providing classified and unclassified presentations.

To report violations, obtain additional information, or schedule a briefing regarding Economic Espionage, contact your local field office at: www.fbi.gov/contact-us/field.

Department of Justice
Federal Bureau of Investigation



Economic Espionage

Protecting America's Trade Secrets

THE FBI SEEKS YOUR HELP IN SAFEGUARDING OUR NATION'S SECRETS!

Our Nation's secrets are in jeopardy, the same secrets that make your company profitable. The FBI estimates billions of US dollars are lost to foreign competitors every year. These foreign competitors deliberately target economic intelligence in advanced technologies and flourishing US industries.

Foreign competitors operate under three categories to create an elaborate network of spies:

1. Aggressively target present and former foreign nationals working for US companies and research institutions;
2. Recruit and perform technical operations to include bribery, discreet theft, dumpster diving (in search of discarded trade secrets) and wiretapping; and,
3. Establish seemingly innocent business relationships between foreign companies and US industries to gather economic intelligence including proprietary information.

In an effort to safeguard our nation's economic secrets, the **Economic Espionage Act (EEA)** was signed into law on October 11, 1996.

WHAT IS ECONOMIC ESPIONAGE TITLE 18 U.S.C., SECTION 1831?

Economic Espionage is (1) whoever knowingly performs targeting or acquisition of trade secrets to (2) knowingly benefit any foreign government, foreign instrumentality, or foreign agent.

WHAT IS THEFT OF TRADE SECRETS TITLE 18 U.S.C., SECTION 1832?

Theft of trade secrets is (1) whoever knowingly performs targeting or acquisition of trade secrets or intends to

WHAT ARE TRADE SECRETS?

Trade secrets are all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, complied, or memorialized physically, electronically, graphically, photographically or in writing, (1) which the owner has taken reasonable measures to protect; and (2) which have an independent economic value from not being generally known to the public.

Commonly referred to as proprietary information, economic policy information, trade information, proprietary technology, or critical technology.

WHAT ARE SOME METHODS OF TARGETING OR ACQUIRING TRADE SECRETS?

1. Steal, conceal, or carry away by fraud, artifice, or deception;
2. Copy, duplicate, sketch, draw, photograph, download, upload, alter, destroy, photocopy, replicate, transmit, deliver, send, mail, communicate, or convey; and,
3. Receive, buy, or possess a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization.

WHO IS A FOREIGN AGENT AND WHAT IS A FOREIGN INSTRUMENTALITY?

A Foreign Agent is any officer, employee, proxy, servant, delegate, or representative of a foreign government. The EEA defines a Foreign Instrumentality as:

Any agency, bureau, ministry, component, institution, association or any legal, commercial or business

ECONOMIC ESPIONAGE ACT OF 1996 PROVISIONS

TERRITORIAL LIMITS

EEA protects against theft that occurs either (1) in the United States, or (2) outside of the United States and (a) an act in furtherance of the offense must have been committed in the United States or (b) the violator is a US person or organization.

CRIMINAL PENALTIES

Title 18 U.S.C., Section 1831 Economic Espionage

- Foreign Government Beneficiary
- Maximum Individual Sentence/Fine: 15 years imprisonment/$5 million.
- Maximum Organizational Fine: Not more than the greater of $10 million or 3 times the value of the stolen trade secret.

Title 18 U.S.C., Section 1832 Theft of Trade Secrets

- Beneficiary must be anyone other than the owner of the misappropriated trade secret(s)
- Maximum Individual Sentence/Fine: 10 years imprisonment/$250,000 or an alternative fine based on gain/loss figures.
- Maximum Organizational Fine: $5 million

CRIMINAL FORFEITURE

The court may order the violator to forfeit to the United States any (1) property constituting, or derived from, any proceeds the person obtained directly or indirectly, as the result of the violation, or (2) property used, or intended to be used, in any manner or part, to commit or facilitate the commission of the violation.

CIVIL PROCEEDINGS

Preventive Measures at Work:

- "Defense in Depth" – use multiple layers of security throughout the computer network.
- Identify ways you have lost data in the past and mitigate those threats. Educate employees about those threats and how to change their behavior, if necessary, to prevent future loss.
- Constantly monitor data movement on your network.
- Establish policies and procedures for intrusion detection systems on company networks.
- Establish policies about what company information can be shared on blogs or personal social web pages. Enforce the policy.
- Educate employees about how their own online behavior could impact the company.
- Provide yearly security training.
- Ask employees to report suspicious incidents as soon as possible.

Additional Preventive Measures:

- Do not store any information you want to protect on any device that connects to the Internet.
- Always use high security settings on social networking sites, and be very limited in the personal information you share. Monitor what others are posting about you on their online discussions.
- Use anti-virus and firewall software. Keep them, your browser, and operating systems patched and updated.
- Change your passwords periodically, and do not reuse old passwords. Do not use the same password for more than one system or service. For example, if someone obtains the password for your email, can they access your online banking information with the same password?
- Do not post anything that might embarrass you later or that you don't want strangers to know

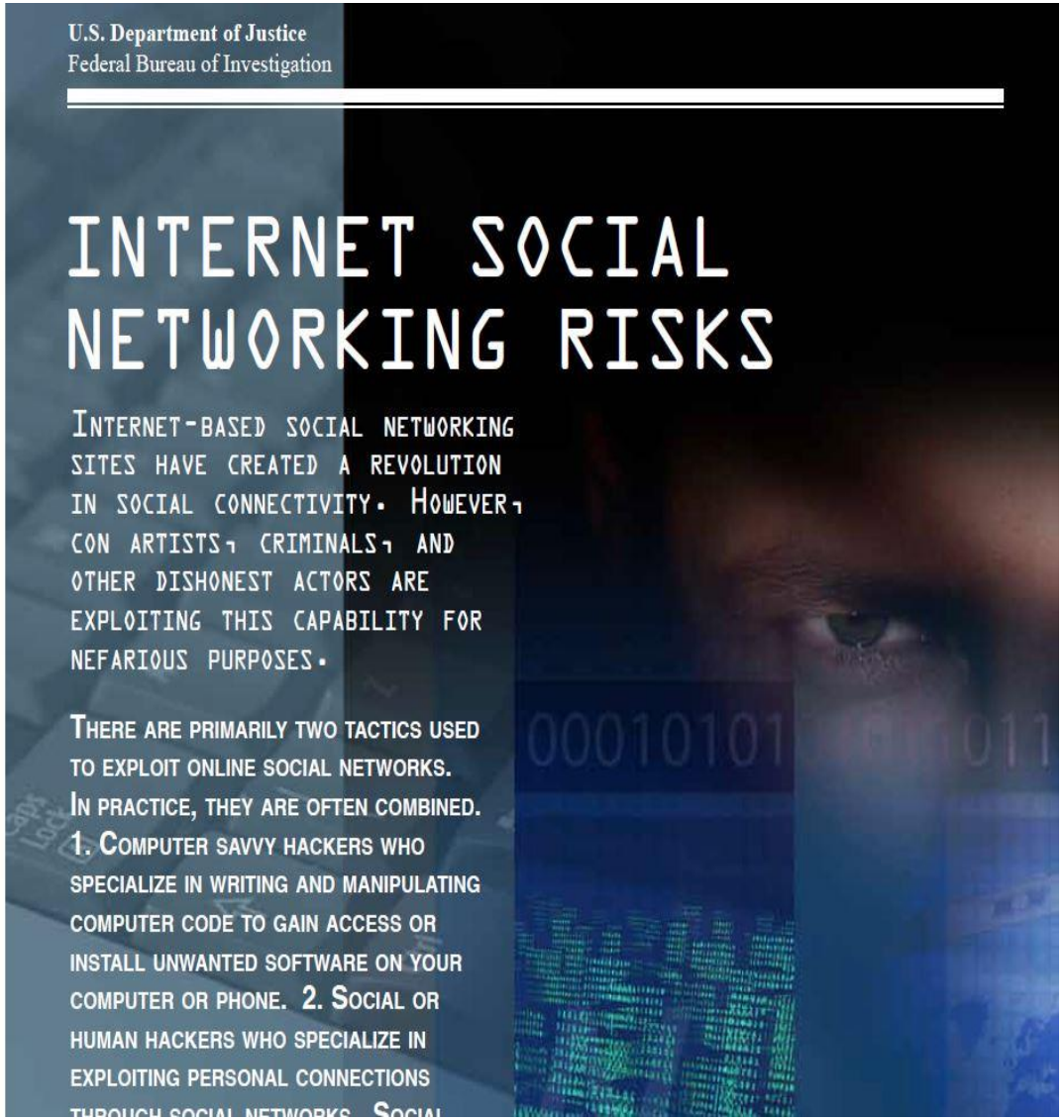
- Disable Global Positioning System (GPS) encoding. Many digital cameras encode the GPS location of a photo when it is taken. If that photo is uploaded to a site, so are the GPS coordinates, which will let people know that exact location.
- Whenever possible, encrypt communications with websites. It may be a feature social network sites allow you to enable.
- Avoid accessing your personal accounts from public computers or through public WiFi spots.
- Beware of unsolicited contacts from individuals in person, on the telephone, or on the Internet who are seeking corporate or personal data.
- Monitor your bank statements, balances, and credit reports.
- Do not share usernames, passwords, social security numbers, credit cards, bank information, salaries, computer network details, security clearances, home and office physical security and logistics, capabilities and limitations of work systems, or schedules and travel itineraries.

> No legitimate service or network administrator will ask you for your password.

- Do not provide information about yourself that will allow others to answer your security questions—such as when using "I forgot my password" feature.
- Be thoughtful and limit personal information you share such as job titles, locations, hobbies, likes and dislikes, or names and details of family members, friends, and co-workers.

Educational Resources:

A number of organizations and websites provide additional details on how to protect you and your workplace from



PURDUE UNIVERSITY
Libraries

FBI Counterproliferation Center

The spread of WMD and other technologies is a significant threat to U.S. national security. That's why the FBI established its Counterproliferation Center (CPC) in 2011. A component of the National Security Branch, the CPC combines the counterproliferation expertise of the Bureau's Counterintelligence Division, WMD Directorate, and Directorate of Intelligence.

FBI Role/Authorities

Although the FBI has the authority to investigate counterproliferation matters under its general criminal jurisdiction, its primary investigative jurisdiction is based on the Bureau's mandate to coordinate all counterintelligence activities within the U.S. (as counterproliferation cases are handled under its counterintelligence program).

The FBI derives its authorities to conduct counterproliferation and export enforcement investigations from the following laws and executive orders:

- **28 CFR 0.85(a):** This law gives the FBI general jurisdiction to investigate violations of all laws, except in cases in which such responsibility is by statute or otherwise exclusively assigned to another investigative agency. As export enforcement laws are not exclusively assigned to any other agency, the FBI is mandated to investigate violations of these laws, including the Arms Export Control Act, International Traffic in Arms Regulations, International Emergency Economic Powers Act, Export Administration Regulations, and Trading with the Enemy Act.
- **28 CFR 0.85(d):** This mandate to take the lead in counterintelligence matters goes back to the FBI's historical authority granted in 1939 by presidential directives to take charge of investigative work in matters relating to espionage, sabotage, subversive activities, and related matters, including investigating potential violations of the Arms Export Control Act, the Export Administration Act, the Trading with the Enemy Act, or the International Economic Powers Act relating to any foreign counterintelligence matter.
- **28 CFR 0.85(l):** This counterterrorism mandate gives the FBI lead agency responsibility in investigating all crimes for which it has primary or concurrent jurisdiction and which involve terrorist activities or acts in preparation of terrorist activities within the statutory jurisdiction of the U.S.
- **28 CFR 0.89:** This law delegates to the FBI Director the authority to seize "arms and munitions of war and other articles" under certain conditions.
- **Executive Order 12333, Section 1.3(b)(20)(A):** This order gives the Director of the FBI authority to coordinate counterintelligence activities inside the United States.
- **Executive Order 12333, Section 1.4(h):** This order requires all members of the U.S. Intelligence Community to coordinate counterintelligence activities in this country with the FBI in accordance with 1.3(b)(20).
- **Executive Order 12333 Section 1.5(g):** This order requires all executive branch agencies to coordinate counterintelligence activities in the U.S. with the FBI in accordance with 1.3(b)(20).

Inside the CPC

The counterproliferation threat facing the U.S. includes ongoing efforts by nation-states to acquire weapons of mass destruction (WMD); the increase of advanced weapons technology worldwide; and attempts by terrorist groups to obtain WMD or advanced weapons technology.

In July 2011, responding to the threat, the FBI combined three counterproliferation-related components into a single jointly-managed entity at FBI Headquarters—the Counterproliferation Center (CPC)—to disrupt global proliferation networks. The three components include:

- The WMD Directorate, which provides scientific expertise;
- The Counterintelligence Division, which provides operational expertise; and
- The Directorate of Intelligence, which provides analytical expertise.

Weapons of Mass Destruction

In July 2006, the FBI created the Weapons of Mass Destruction (WMD) Directorate to build a cohesive and coordinated approach to incidents involving chemical, biological, radiological, or nuclear (CBRN) material—with an overriding focus on prevention. The WMD Directorate proactively seeks out and relies on intelligence to drive preparedness, countermeasures, and

WMD Basics

Definition of WMD

Title 18 U.S.C. §2332a defines weapons of mass destruction (WMD) as:

- Any explosive, incendiary, or poison gas, including the following: a bomb; grenade; rocket having an explosive or incendiary charge of more than four ounces; missile having an explosive or incendiary charge of more than one-quarter ounce; mine; or device similar to any of the previously described devices;
- Any weapons that is designed or intend to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors;
- Any weapon involving a disease organism; and
- Any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.

Nature of the Threat

According to national policy, WMD refers to materials, weapons, or devices that are intended to cause (or are capable of causing) death or serious bodily injury to a significant number of people through release, dissemination, or impact of toxic or poisonous chemicals or precursors, a disease organism, or radiation or radioactivity, including (but not limited to) biological devices, chemical devices, improvised nuclear devices, radiological dispersion devices, and radiological exposure devices.

WMD terrorism and proliferation are evolving U.S. national security threats. The Director of National Intelligence has stated that dozens of identified domestic and international terrorists and terrorist groups have expressed their intent to obtain and use WMD—including nuclear materials. Indicators of this increasing threat include the 9/11 attacks, the Amerithrax letters, and multiple attempts by terrorists at home and abroad to use improvised explosives created from basic chemical precursors. The challenge presented by these threats is compounded by the large volume of hoax threats that distract and divert law enforcement agencies from addressing real threats.

Inside Our Operations

The WMD Directorate exists to ensure the FBI and partners are prepared to anticipate, mitigate, disrupt, or respond to WMD threats. With the continued evolution of the WMD threat and the possibility of an overseas origin or nexus, the Directorate advances WMD prevention activities by supporting international WMD capacity building, developing plans and policies at strategic and operational levels, developing partnerships, training, and conducting outreach endeavors. By improving WMD security on a global level, the Directorate protects U.S. interests abroad and keeps WMD threats outside our borders.

At the field office level—and at select legal attaché offices overseas—the WMD Directorate conducts prevention and outreach efforts through Bureau agents who serve as WMD coordinators. These coordinators regularly meet with representatives from industry and academic institutions, public health officials, local law enforcement, and first responders to raise awareness about threats to our national security. These efforts are known as **setting tripwires**, and the intent is to establish an early-warning network where those who are aware of an emerging situation know the potential risks and are prepared to inform the FBI when suspicions are raised.

FBI VAULT HTTPS://VAULT.FBI.GOV/

- Features over 6,700 documents and other media containing selected historic FBI mission records. Categories covered include:
- Bureau Personnel
- Counterterrorism
- Foreign Counterintelligence
- Fugitives
- Organizations
- Organized Crime
- Political Figures
- Popular Culture
- Public Corruption
- Violent Crime
- World War II

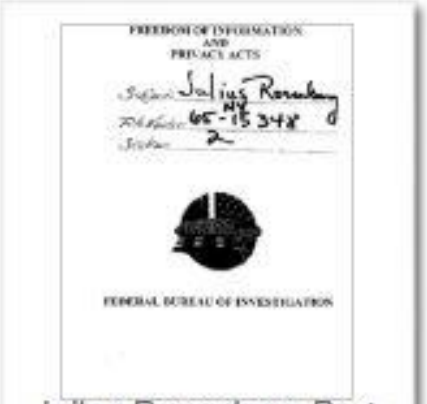
PURDUE UNIVERSITY
Libraries

JULIUS ROSENBERG (1918-1953) ARMY SIGNAL CORPS EMPLOYEE AND COMMUNIST PARTY MEMBER CONVICTED OF PASSING NUCLEAR SECRETS TO SOVIET UNION. EXECUTED JUNE 19, 1953.

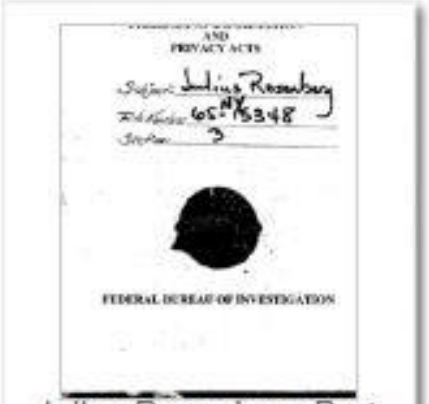
Julius Rosenberg

Search...

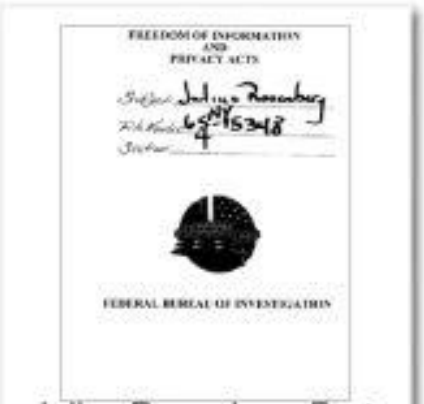
Julius Rosenberg Part 01 of 87



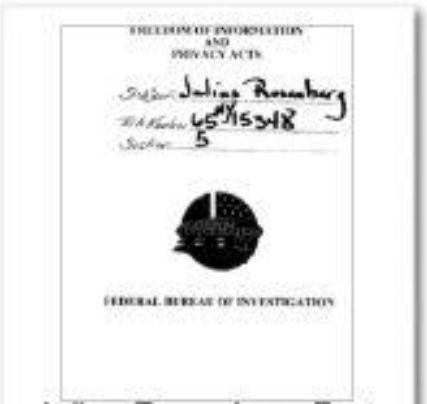
Julius Rosenberg Part 02 of 87



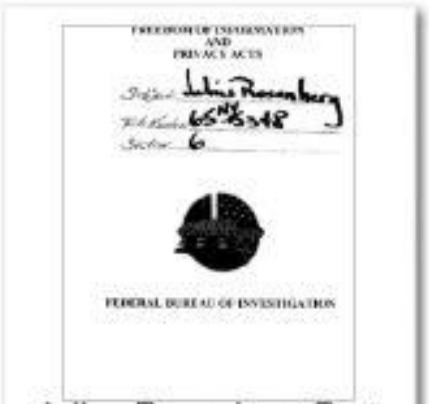
Julius Rosenberg Part 03 of 87



Julius Rosenberg Part 04 of 87



Julius Rosenberg Part 05 of 87



Julius Rosenberg Part 06 of 87

PURDUE UNIVERSITY
Libraries

FREEDOM OF INFORMATION AND PRIVACY ACTS

Subject: Julius Rosenberg

File Number: NY 65-15345

Section: 14

Mr. LOUIS FISHER, 226 Lafayette Street, New York City, advised that his firm has maintained business connections with the Pitt Machine Products Inc. for the past four years but that he knows nothing concerning the private affairs of Mr. JULIUS ROSENBERG. Mr. FISHER further stated that his files contain an average of from 50 to 100 invoices for each of the four years for equipment in common usage in the machine tool industry. Mr. FISHER said that he would hold ROSENBERG's entire invoice record in his file for the New York Office until such time as it may be needed. FISHER further added that he knew GREENGLASS very slightly through his business connections with the firm.

Mr. J. BERNSTEIN, electrician, 170 Rivington Street, New York City, advised that he has been acquainted with the GREENGLASS family for the past twenty years since they live only a few doors from his place of business. Mr. BERNSTEIN said he knew nothing about the personal activities of the family and was surprised when he read of GREENGLASS' arrest. BERNSTEIN further added that he wired the building used by the Pitt Machine Products Corporation on East Third Street and the building which is presently occupied on East Houston Street, and that this is his only business connection with the firm. Mr. BERNSTEIN said that he knew GREENGLASS' father, BARNET, and that BARNET had been engaged in the sewing machine business but that they had had very limited business connections.

Inquiry on East 21 Street, New York City, failed to reflect any such number as 263, which was supposed to have been occupied by the Orlick

Usama (Osama) Bin Laden

Usama (or Osama) Bin Laden, founder of the al Qaeda terrorist organization, was born in Saudi Arabia in 1957. On March 10, 1984, Bin Laden and others killed two German nationals. On March 16, 1998, authorities in Tripoli issued an arrest warrant for him for murder and illegal possession of firearms. Bin Laden was also wanted for the August 1998 bombing of U.S. embassies in Kenya and Tanzania. He was killed by U.S. forces in May 2011. This release consists of material that predates the 9/11 attacks.

Search...

Osama Bin Laden Part 01 of 03

Osama Bin Laden Part 02 of 03

Osama Bin Laden Part 03 of 03

DATE AND PLACE OF BIRTH: 1957 - Jeddah, Saudi Arabia

FATHER'S FORENAMES: Abdulrahamn 'Awadh

IDENTITY CONFIRMED - NATIONALITY: SAUDI ARABIAN (CONFIRMED)

LANGUAGE SPOKEN: Arabic.

ACCOMPLICES:

AL-'ALWAN Faraj Mikhaïl Abdul-Fadeel Jibril, born in 1969, subject of red notice File No. 1998/20220, Control No. A-270/5-1998;

AL-WARFALI Faez Abu Zeid Muftah, born in 1968, subject of red notice File No. 1998/20223, Control No. A-271/5-1998;

AL-CHALABI Faraj, born in 1966, subject of red notice File No. 1998/20230, Control No. A-269/5-1998.

SUMMARY OF FACTS OF THE CASE: LIBYA: On 10th March 1994, BIN LADEN, AL-CHALABI, AL-'ALWAN and AL-WARFALI killed two German nationals near Surt.

REASON FOR NOTICE: Wanted on arrest warrant No. 1.27.288/1998, issued on 16th March 1998 by the judicial authorities in Tripoli, Libya, for murder and illegal possession of firearms.

authorizing his followers to commit violent acts against the U.S. In February, 1998 BIN LADEN endorsed a fatwah authorizing the killing of American civilians anywhere in the world where they can be found. The substance of these were repeated by Bin Laden during a press conference in May, 1998. During July and August, 1998 members of "al Qaeda" made preparations to detonate explosives near the U.S. embassies in Kenya and Tanzania. The embassies were actually bombed on 7 August 1998. More than 216 lives were lost in the Kenya explosion and more than 10 lives were lost in the explosion in Tanzania.

2.2 ACCOMPLICES:

Muhammad Atef; Wadih El Hage; Mohamed Sadeek Odeh; Mohamed Rashed Daoud Al-Owhali; Mustafa Mohamed Fadhil; Khalfan Khamis Mohamed; Ahmed Khalfan Ghailani; Sheikh Ahmed Salim Swedan;Msalam, f/n Fahid, Mohammed Ally

2.3 CHARGE:

Murder; Murder Conspiracy; Attack on a United States Facility

2.4 LAW COVERING THE OFFENCE:

Title 18 United States Code Sections 2332(b), 844(f) and 930(a)

COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION (CCIPS)

ABOUT THE COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION

The Computer Crime and Intellectual Property Section (CCIPS) is responsible for implementing the Department's national strategies in combating computer and intellectual property crimes worldwide. CCIPS prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts. Section attorneys work to improve the domestic and international infrastructure-legal, technological, and operational-to pursue network criminals most effectively. The Section's enforcement responsibilities against intellectual property crimes are similarly multi-faceted. Intellectual Property (IP) has become one of the principal U.S. economic engines, and the nation is a target of choice for thieves of material protected by copyright, trademark, or trade-secret designation. In pursuing all these goals, CCIPS attorneys regularly run complex investigations, resolve unique legal and investigative issues raised by emerging computer and telecommunications technologies; litigate cases; provide litigation support to other prosecutors; train federal, state, and local law enforcement personnel; comment on and propose legislation; and initiate and participate in international efforts to combat computer and intellectual property crime.

GENERAL INFORMATION
COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION

LEADERSHIP

John Lynch
Chief, Computer Crime & Intellectual Property Section

CONTACT

Department of Justice Main Switchboard
(202) 514-2000

AN IMPORTANT COURT OPINION HOLDS LAWFUL WARRANTS CAN BE USED TO OBTAIN EVIDENCE FROM U.S. INTERNET SERVICE PROVIDERS WHEN THOSE PROVIDERS STORE EVIDENCE OUTSIDE THE U.S.

February 6, 2017

Courtesy of Acting Assistant Attorney General Kenneth Blanco

On Friday, a United States Magistrate Judge in the Eastern District of Pennsylvania issued an important opinion in a dispute between the United States and Google over whether Google must comply with warrants issued by United States judges. The matter involved two warrants to search Google accounts belonging to suspected criminals in the United States who communicated with others in the United States. Google refused to fully comply with the warrants, asserting that it could not be compelled to disclose data unless it knew the data was actually located in the United States. The Magistrate Judge ordered Google to comply with the search warrants, specifically finding that no seizure occurs outside the United States and that the search occurs in Pennsylvania.

As background: When the government has probable cause to believe that an e-mail account contains evidence of a crime, it can apply for a search warrant from a federal court. If a judge finds that the government has shown probable cause, that judge then issues a search warrant to the e-mail provider to produce the data. The search warrant is then served on an e-mail provider (such as Google or Microsoft), who then must, under law, produce to the government the e-mails that the warrant describes. The government's ability to do this is critical to criminal investigations into crimes as varied as fraud, computer hacking, terrorism, murder, kidnapping, organized crime, sexual abuse or exploitation of children, identity theft and more.

Friday's opinion involved an investigation of crimes that occurred in the United States, were committed by United States citizens, and were committed against United States victims. Those crimes were facilitated by e-mails sent inside the United States to recipients also inside the United States. But Google only partially complied with the search warrants, refusing to produce all of the information in its possession, custody and control. Google instead limited its production to records that it said it could determine were stored within the United States.

Best Practices for Victim Response and Reporting of Cyber Incidents[1]

Version 2.0 (September 2018)

Any Internet-connected organization can fall prey to a disruptive network intrusion or costly cyber attack. A quick, effective response to a cyber incident can be critical to minimizing the resulting harm and expediting recovery. The best time to plan such a response is now, *before* a data breach incident, ransomware attack, or other cyber incident occurs.

The Cybersecurity Unit originally published this "best practices" document to help organizations prepare a cyber incident response plan and, more generally, to better equip themselves to respond effectively and lawfully to a cyber incident. This updated version includes additional incident response considerations, including ransomware, information sharing pursuant to the Cybersecurity Information Sharing Act of 2015, cloud computing, and working with cyber incident response firms. It distills lessons learned by federal investigators and prosecutors and input from private sector companies that have managed cyber incidents. It includes advice on preventing cyber incidents, as well as advice on working effectively with law enforcement. Like its predecessor, it was drafted primarily for smaller organizations and their legal counsel; however, it may be useful for larger organizations with more experience in handling cyber incidents as well.

I. Steps to Take *Before* a Cyber Intrusion or Attack Occurs

SUPPORTING INNOVATION, CREATIVITY & ENTERPRISE

CHARTING A PATH AHEAD

U.S. JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT

FY 2017 - 2019

PURDUE UNIVERSITY
Libraries

1. Promote Necessary Seizure Authority and Best Practices Around the World.

Each nation should endeavor to maximize its effectiveness at interdicting illicit goods. By adopting modern and effective interdiction authorities, international customs organizations will be able to conduct enforcement operations consistent with international norms. The United States and the WCO, for example, have long advocated for development of model legislation and best practices, but progress has been slow.[27] Two key subject matter areas that present a material opportunity for improvement are: (1) the implementation of *ex officio* authority, and (2) the confirmation that the clearance of goods includes those that are moving *in transit*.

Ex Officio Authority.

The ability of customs officers to act *ex officio* in interdicting infringing goods is critical to our success in curbing illicit trade. As recognized by the WCO:

is inadequate for at least two reasons.

First, the rights holder may not have adequate resources to initiate an action in each and every implicated country, city, or port around the world. Unfortunately, the absence of actual *ex officio* authority in law (and applied in practice) is not limited to a small subset of nations, but rather, appears to be the norm for large segments of the world. Small and medium enterprises, for example, generally do not have the infrastructure in place to be responsive to customs-based inquiries the world over, especially within the allocated window of time (*i.e.*, generally 3-5 days). Even with a large, multinational company, the scope of global trade and container port throughput is so vast, that few if any companies can reasonably respond to all trade inquiries in a timely manner. There are over 100 ports in Latin America and the Caribbean alone, with the container port throughput for the top 20 ports (*FIG. 53)* in this region at approximately 48 million TEU (a standard unit of measurement, with each TEU equivalent to a

FARA

Foreign Agents Registration Act

The Foreign Agents Registration Act (FARA) was enacted in 1938. FARA is a disclosure statute that requires persons acting as agents of foreign principals in a political or quasi-political capacity to make periodic public disclosure of their relationship with the foreign principal, as well as activities, receipts and disbursements in support of those activities. Disclosure of the required information facilitates evaluation by the government and the American people of the statements and activities of such persons in light of their function as foreign agents. The FARA Registration Unit of the Counterintelligence and Export Control Section (CES) in the National Security Division (NSD) is responsible for the administrative enforcement of the Act.

FARA CONTACT INFORMATION

GENERAL INFORMATION
NATIONAL SECURITY DIVISION

LEADERSHIP

John C. Demers
Assistant Attorney General for National Security

CONTACT

Legal authorities: 28 USC 611 & 28 CFR 5

October 2, 2018

[Adressee deleted]

Re: Possible Obligation to Register under the Foreign Agents Registration Act

Dear [name deleted]:

This is in reference to your email message of September 6, 2018, in which you request an advisory opinion, pursuant to 28 C.F.R. § 5.2, regarding your possible obligation to register pursuant to the Foreign Agents Registration Act of 1938, as amended, 22 U.S.C. § 611 *et seq.* ("FARA" or the "Act").

In your message you informed us that you are negotiating with [U.S. law firm], a law firm in [the United States], to assist [U.S. law firm] in its representation of [foreign company], in making a voluntary self-disclosure to the Office of Export Enforcement at the Department of Commerce ("OEE"). You indicate that your assistance would consist of disclosing not only [foreign company]'s own unlicensed re-exports to [foreign country] in violation of the Export Administration Regulations, but also the possible violations of other foreign and domestic entities that may also have engaged in unlicensed re-exports to [foreign country]. You informed us that you would work with [U.S. law firm] and [foreign company] to review documents and possibly prepare and make a presentation to OEE concerning the mitigating factors in the investigation of the competitors and other involved companies. We thank you for attaching a copy of the proposed engagement agreement for review.

After careful consideration of the facts presented to us in your message and the contract

FARA DOCUMENT SEARCH

This is an initial release of the FARA document search tool, providing Internet access to the vast majority of public documents on file with the FARA Registration Unit. However, because some potential privacy issues remain under review, there are certain FARA documents not available via the Internet at this time, but which still can be accessed at the FARA public office. Feedback and suggestions from the general public are encouraged and can be submitted by clicking on the following link: Provide Feedback

Document Search Help

* denotes required field

*Document Type ALL *Status ALL

Registrant Number

Registrant Name ==> Exact Sounds like

Stamped/Received Date Start End

Search Reset

PURDUE UNIVERSITY
Libraries

OMB No. 1124-0002; Expires May 31, 2020

U.S. Department of Justice

Washington, DC 20530

Supplemental Statement Pursuant to the Foreign Agents Registration Act of 1938, as amended

For Six Month Period Ending 10/31/2018

(Insert date)

I - REGISTRANT

1. (a) Name of Registrant

China Daily Distribution Corp.

(b) Registration No.

3457

(c) Business Address(es) of Registrant

1500 Broadway Ste 2800, New York, NY 10036

U.S. Department of Justice
Washington, D.C. 20530

Dissemination Report

OMB No. 1105-0006

INSTRUCTIONS: Report must be submitted in duplicate to the Registration Unit, Internal Security Section, Criminal Division, Department of Justice, Washington, D.C. 20530. The original must be signed by or on behalf of the registrant. All items in this form must be answered, unless the answer is "none" or "not applicable," in which case such an entry shall be made in the appropriate space. If additional space is needed for any item, attach supplemental sheet identifying each item.

1. Name of registrant
Korea Trade Promotion Center

2. Registration No.
1619

3. Nature of material *(A concise account of the nature of the propaganda material filed)*
Magazine and newsletter reporting on Korean business and economy; Korean products available for purchase; information on Expo '93

4. Title of material, if any
KOTRA Trade News; Korea Trade & Business; Korea Trade; Expo '93

5. Name of foreign principal on whose behalf this material was transmitted.
Korea Trade Promotion Corp.
Seoul, Korea

6. Means of transmission
Mail or by Hand

7. Dates of transmission
21st of each month

8. Total copies transmitted
200 each

9. List addresses from which this material was transmitted:
Korea Trade Promotion Center
460 Park Avenue
New York, N.Y. 10022

10. List states and territories of the United States to which material was transmitted:
Maine, New Hampshire, Vermont, Mass., Rhode Island, Conn., N.Y. Penna., N.J., Del., Maryland, Virginia, & West Virginia

11. Types of recipients *(Give number of organizations in each group)*

Libraries
Public officials 18
Newspapers 7
Press services of associations
Educational institutions
Civic groups 1
Other *(specify)* U.S. businesses (1000)

12. List names and addresses of persons or organizations receiving 100 copies or more:
Copies limited to one per person or organization

13. If the material transmitted was a film or radio or television script, furnish the following information:

Name of station, organization, or theater using *(including city and state)*	Date or dates broadcast or shown	Estimated attendance (for film(s))
- Not applicable -		

RECEIVED
DEPT. OF JUSTICE
CRIMINAL DIVISION
'91 DEC -6 A10:11
INTERNAL SECURITY
SECTION
REGISTRATION UNIT

14. Have two copies of this material been filed with the Department of Justice? Yes ☐ No ☐

15. Has this material been labeled as required by the act? Yes ☐ No ☐

Date of report	Name and title	Signature
Nov. 1991	Yong Jip Kim, Executive Director	Y. J. K.

Formerly OBD-69

FORM CRM-159
FEB. 84

OMB No. 1124-0001, Expires May 31, 2020

U.S. Department of Justice

Washington, DC 20530

Registration Statement
Pursuant to the Foreign Agents Registration Act of 1938, as amended

I--REGISTRANT

1. Name of Registrant

2. Registration No. (To Be Assigned By the FARA Registration Unit)

3. Principal Business Address

4. If the registrant is an individual, furnish the following information:

   (a) Residence address(es)

During the period beginning 60 days prior to the date of your obligation to register[6] to the time of filing this statement, did you spend or disburse any money in furtherance of or in connection with your activities on behalf of any foreign principal named in Item 7? Yes ☐ No ☐

If yes, set forth below in the required detail and separately for each such foreign principal named including monies transmitted, if any, to each foreign principal.

Date	To Whom	Purpose	Amount

(b) **DISBURSEMENTS-THINGS OF VALUE**

During the period beginning 60 days prior to the date of your obligation to register[7] to the time of filing this statement, did you dispose of any thing of value[8] other than money in furtherance of or in connection with your activities on behalf of any foreign principal named in Item 7? Yes ☐ No ☐

If yes, furnish the following information:

Date	Recipient	Foreign Principal	Thing of Value	Purpose

15. Activities in preparing or disseminating informational materials will include the use of the following:

- ☐ Radio or TV broadcasts
- ☐ Magazine or newspaper
- ☐ Motion picture films
- ☐ Letters or telegrams
- ☐ Advertising campaigns
- ☐ Press releases
- ☐ Pamphlets or other publications
- ☐ Lectures or speeches
- ☐ Other *(specify)* _____

Electronic Communications

- ☐ Email
- ☐ Website URL(s): _____
- ☐ Social media website URL(s): _____
- ☐ Other *(specify)* _____

16. Informational materials will be disseminated among the following groups:

- ☐ Public officials
- ☐ Legislators
- ☐ Government agencies
- ☐ Newspapers
- ☐ Editors
- ☐ Civic groups or associations
- ☐ Libraries
- ☐ Educational groups
- ☐ Nationality groups
- ☐ Other *(specify)* _____

Report of the Attorney General to the Congress of the United States on the Administration of the Foreign Agents Registration Act of 1938, as amended, for the six months ending December 31, 2017

Endeavor Law Firm, PC #5934

1775 Pennsylvania Avenue, NW
Washington, DC 20006

Deripaska, Oleg

Nature of Services: Promotion of Trade

The registrant provided general legal advice regarding legislative, trade, foreign policy, investment, security, and investigated joint business opportunities in the energy industry in the United States including biofuels and natural gas.

$273,661.58 for the six month period ending November 30, 2017

Manatos & Manatos #6353

1100 New Hampshire Avenue, NW
Washington, DC 20037

VTB Group

Nature of Services: Lobbying

The registrant provided on behalf of the foreign principal government strategies counsel and arranged meetings with U.S. policymakers regarding the imposition of sanctions by the United States Government.

$52,500.00 for the six month period ending November 30, 2017

Reston Translator, LLC #6490

11140 Glade Street
Reston, VA 20191

Federal State Unitary Enterprise Rossiya Segodnya International Information Agency

2005

- FARA Second Semi-Annual Report - 2005
- FARA First Semi-Annual Report - 2005

2004

- FARA Second Semi-Annual Report - 2004
- FARA First Semi-Annual Report - 2004

2003

- FARA Second Semi-Annual Report - 2003
- FARA First Semi-Annual Report - 2003

2002

- FARA Second Semi-Annual Report - 2002
- FARA First Semi-Annual Report - 2002

2001

- FARA Second Semi-Annual Report - 2001
- FARA First Semi-Annual Report - 2001

1942-2000

- FARA Reports to Congress - Archives

UNITED STATES
Foreign Intelligence Surveillance Court

Search

Home | About the Court | Rules of Procedure | Public Filings | Judges | Correspondence | Court of Review | Amici Curiae

Public Filings »

The Foreign Intelligence Surveillance Court was established by Congress in 1978. The Court entertains applications made by the United States Government for approval of electronic surveillance, physical search, and certain other forms of investigative actions for foreign intelligence purposes.

Recent Public Filings

- Motion of Thomas C. Goldstein For Appointment As Amicus Curiae and For Leave to File Amicus Curiae Brief
  Case/Docket: Misc. 18-04
  Date Posted: *Tuesday, December 11, 2018*
- Movants' Reply Brief In Response to the Court's Order of May 1, 2018
  Case/Docket: Misc. 13-08
  Date Posted: *Thursday, August 2, 2018*

Annual Reports

ESTABLISHED IN 1978 WITH ENACTMENT OF FOREIGN INTELLIGENCE SURVEILLANCE ACT P.L. 95-511 50 USC 1801-1885C

- Based in Washington, DC. Consists of 11 federal district court judges designated by Supreme Court Chief Justice.
- Each judge serves maximum seven years and terms are staggered to ensure continuity.
- Judges must come from at least 7 U.S. judicial circuits and three judges must live within 20 miles of Washington, DC.
- Judges typically sit for one week at a time on a rotating basis.
- Court reviews electronic surveillance, physical search, and investigative actions for foreign intelligence purposes.
- Court work occurs ex parte with only one party knowing and the other party not knowing or participating. This is due to the need to protect classified national security information.

UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT
Washington, D.C.

RULES OF PROCEDURE
Effective November 1, 2010

Rule **Page**

Title I. Scope of Rules; Amendment

Title II. National Security Information

Rule 12. Submission of Targeting and Minimization Procedures. In a matter involving Court review of targeting or minimization procedures, such procedures may be set out in full in the government's submission or may be incorporated by reference to procedures approved in a prior docket. Procedures that are incorporated by reference to a prior docket may be supplemented, but not otherwise modified, in the government's submission. Otherwise, proposed procedures must be set forth in a clear and self-contained manner, without resort to cross-referencing.

FOREIGN INTELLIGENCE SURVEILLANCE COURT
FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW
Current and Past Members
May 2018

Brotman	Stanley	S.	3	NJ	FISC	07/17/1997	05/18/2004
Bryan	Albert	V.	4	VA Eastern	FISC	01/01/1979	01/01/1986
Bryson	William	Curtis	Federal		FISCR	12/1/2011 Presiding 9/1/2013	05/18/2018
Cabranes	José	A.	2		FISCR	08/09/2013 Presiding 05/19/2018	05/18/2020
Cacheris	James	C.	4	VA Eastern	FISC	09/10/1993	05/18/2000
Carr	James	G.	6	OH Northern	FISC	05/19/2002	05/18/2008
Carroll	Earl	H.	9	AZ	FISC	02/23/1993	05/18/1999
Coffman	Jennifer	B.	6th	KY - Eastern	FISC	05/19/2011	01/08/2013
Collyer	Rosemary	M.	DC	DC	FISC	03/08/2013 Presiding 05/19/2016	03/07/2020
Contreras	Rudolph		DC	DC	FISC	05/19/2016	05/18/2023
Conway	Anne	C.	11th	FL – Middle	FISC	05/19/2016	05/18/2023

Kugler, Robert B.

Born 1950 in Camden, NJ

Federal Judicial Service:
Judge, U.S. District Court for the District of New Jersey
Nominated by George W. Bush on August 1, 2002, to a seat vacated by Joseph E. Irenas. Confirmed by the Senate on November 14, 2002, and received commission on December 4, 2002. Assumed senior status on November 2, 2018.

Other Federal Judicial Service:
U.S. Magistrate Judge, U.S. District Court for the District of New Jersey, 1992-2002
Judge, Foreign Intelligence Surveillance Court, 2017-present

Education:
Syracuse University, B.A., 1975
Rutgers School of Law -- Camden, J.D., 1978

Professional Career:
Law clerk, Hon. John F. Gerry, U.S. District Court, District of New Jersey, 1978-1979
Assistant prosecutor, Camden County, New Jersey, 1979-1981
Deputy attorney general, State of New Jersey, 1981-1982
Private practice, New Jersey, 1982-1992

Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

I am writing in response to your letter of July 18, 2013, in which you posed several questions about the operations of the Foreign Intelligence Surveillance Court (the Court). As you requested, we are providing unclassified responses. We would note that, as a general matter, the Court's practices have evolved over time. Various developments in the last several years – including statutory changes, changes in the size of the Court and its staff, the adoption of new Rules of Procedure in 2010, and the relocation of the Court's facilities from the Department of Justice headquarters to a secure space in the federal courthouse in 2009 – have affected some of these practices. The responses below reflect the current practices of the Court.

1. *Describe the typical process that the Court follows when it considers the following: (1) an application for an order for electronic surveillance under Title I of FISA; (2) an application for an order for access to business records under Title V of FISA; and (3) submissions from the government under Section 702 of FISA. As to applications for orders for access to business records under Title V of FISA, please describe whether the process for the Court's consideration of such applications is different when considering requests for bulk collection of phone call metadata records, as recently declassified by the Director of National Intelligence.*

Each week, one of the eleven district court judges who comprise the Court is on duty in Washington. As discussed below, most of the Court's work is handled by the duty judge with the assistance of attorneys and clerk's office personnel who staff the Court. Some of the Court's more complex or time-consuming matters are handled by judges outside of the duty-week system, at the discretion of the Presiding Judge. In either case, matters before the Court are thoroughly reviewed and analyzed by the Court.

3. *Public FISA Court opinions and orders make clear that the Court has considered the views of non-governmental parties in certain cases, including a provider challenge to the Protect America Act of 2007. Describe instances where non-governmental parties have appeared before the Court. Has the Court invited or heard views from a nongovernmental party regarding applications or submissions under Title I, Title V, or Title VII of FISA? If so, how did this come about, and what was the process or mechanism that the Court used to enable such views to be considered?*

FISA does not provide a mechanism for the Court to invite the views of nongovernmental parties. In fact, the Court's proceedings are *ex parte* as required by the statute (see, e.g., 50 U.S.C. §§ 1805(a), 1824(a), 1842(d)(1) & 1861(c)(1)), and in keeping with the procedures followed by other courts in applications for search warrants and wiretap orders. Nevertheless, the statute and the FISC Rules of Procedure provide multiple opportunities for recipients of Court orders or government directives to challenge those orders or directives, either directly or through refusal to comply with orders or directives. Additionally, as detailed below, there have been several instances – particularly in the past several months – in which nongovernmental parties have appeared before the Court outside of the context of a challenge to an individual Court order or government directive.

There has been one instance in which the Court heard arguments from a nongovernmental party that sought to substantively contest a directive from the government. Specifically, in 2007, the government issued directives to Yahoo!, Inc. (Yahoo) pursuant to Section 105B of the Protect America Act of 2007 (PAA). Yahoo refused to comply with the directives, and the government

---

[9] This assessment does not include minor technical or typographical changes, which occur more frequently.

Amici Curiae

Individuals Designated as Eligible to Serve as an Amicus Curiae Pursuant to 50 U.S.C. § 1803(i)(1)

Name	Title	Organization
Effective November 25, 2015:		
Jonathan G. Cedarbaum	Partner	Law Firm of WilmerHale (Washington D.C. office)
Laura Donohue	Professor of Law	Georgetown Law
Amy Jeffress	Partner	Law Firm of Arnold & Porter (Washington D.C office)
Marc Zwillinger	Managing member	ZwillGen PLLC (Washington D.C.)
Effective March 31, 2016:		
David S. Kris	Co-Founder	Culper Partners LLC
Effective October 1, 2018:		
Ana I. Anton, Ph.D	Professor	School of Interactive Computing, Georgia Institute of Technology
Ben Johnson	Co-Founder and CTO	Obsidian Security
Robert T. Lee	Digital Forensics and Incident Response Lead	SANS Institute

UNITED STATES FOREIGN
INTELLIGENCE SURVEILLANCE COURT
Washington, D.C.

onorable Rosemary M. Collyer
Presiding Judge

February 15, 2018

Honorable Devin Nunes
Chairman
Permanent Select Committee on Intelligence
United States House of Representatives
Washington, D.C. 20515

Dear Chairman Nunes:

I write in response to your letter of February 7, 2018, in which you request that the Foreign Intelligence Surveillance Court confirm whether "transcripts of relevant FISC hearings associated with" matters described in the letter exist and, if so, provide copies to the Committee. As you know, any such transcripts would be classified. It may also be helpful for me to observe that, in a typical process of considering an application, we make no systematic record of questions we ask or responses the government gives.

The Court appreciates the interest of the House Intelligence Committee in its operations and public confidence therein. Before 2018, the Court had never received a request from

Congress for documents related to any specific FISA application. Thus, your requests – and others I have recently received from Congress – present novel and significant questions. The considerations involve not only prerogatives of the Legislative Branch, but also interests of the Executive Branch, including its responsibility for national security and its need to maintain the integrity of any ongoing law enforcement investigations.

While this analysis is underway, you may note that the Department of Justice possesses (or can easily obtain) the same responsive information the Court might possess, and because of separation of powers considerations, is better positioned than the Court to respond quickly. (We have previously made clear to the Department, both formally and informally, that we do not object to any decision by the Executive Branch to convey to Congress any such information.)

We have asked the Executive Branch to keep us informed regarding any information concerning the FISC that it provides to Congress. If you choose to present your request to the Executive Branch, we likewise request that you kindly let us know.

Sincerely,

Rosemary M. Collyer
Presiding Judge

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

2018 JUL 25 PM 2:53

LEEANN FLYNN HALL
CLERK OF COURT

IN RE TRANSCRIPTS OF THIS COURT RELATED TO THE SURVEILLANCE OF CARTER PAGE	)	Docket No. Misc. 18-03

JUDICIAL WATCH, INC.'S MOTION
FOR PUBLICATION OF COURT TRANSCRIPTS

Plaintiff Judicial Watch, Inc., by counsel and pursuant to Rule 62 of the Rules of Procedure for the Foreign Intelligence Surveillance Court, respectfully requests this Court make public all transcripts of hearings regarding applications for or renewal of Foreign Intelligence Surveillance Act warrants related to Carter Page. As grounds therefor, Plaintiff states as follows:

I. Introduction.

Earlier this year, the House Permanent Select Committee on Intelligence requested this Court confirm whether transcripts of hearings related to Carter Page exist and, if so, to provide copies of such transcripts to the Committee. In response, the Court informed the Select Committee "that the Department of Justice possesses (or can easily obtain) the same responsive

February 2, 2018

The Honorable Devin Nunes
Chairman, House Permanent Select Committee on Intelligence
United States Capitol
Washington, DC 20515

Dear Mr. Chairman:

On January 29, 2018, the House Permanent Select Committee on Intelligence (hereinafter "the Committee") voted to disclose publicly a memorandum containing classified information provided to the Committee in connection with its oversight activities (the "Memorandum," which is attached to this letter). As provided by clause 11(g) of Rule X of the House of Representatives, the Committee has forwarded this Memorandum to the President based on its determination that the release of the Memorandum would serve the public interest.

The Constitution vests the President with the authority to protect national security secrets from disclosure. As the Supreme Court has recognized, it is the President's responsibility to classify, declassify, and control access to information bearing on our intelligence sources and methods and national defense. *See, e.g., Dep't of Navy v. Egan*, 484 U.S. 518, 527 (1988). In order to facilitate appropriate congressional oversight, the Executive Branch may entrust classified information to the appropriate committees of Congress, as it has done in connection with the Committee's oversight activities here. The Executive Branch does so on the assumption that the Committee will responsibly protect such classified information, consistent with the laws of the United States.

protect the information. The White House review process also included input from the Office of the Director of National Intelligence and the Department of Justice. Consistent with this review and these standards, the President has determined that declassification of the Memorandum is appropriate.

Based on this assessment and in light of the significant public interest in the memorandum, the President has authorized the declassification of the Memorandum. To be clear, the Memorandum reflects the judgments of its congressional authors. The President understands that oversight concerning matters related to the Memorandum may be continuing. Though the circumstances leading to the declassification through this process are extraordinary, the Executive Branch stands ready to work with Congress to accommodate oversight requests consistent with applicable standards and processes, including the need to protect intelligence sources and methods.

Sincerely,

Donald F. McGahn II
Counsel to the President

cc: The Honorable Paul Ryan
Speaker of the House of Representatives

The Honorable Adam Schiff
Ranking Member, House Permanent Select Committee on Intelligence

Director's Report on Foreign Intelligence Surveillance Courts' Activities

This report contains statistics reported by the Foreign Intelligence Surveillance Court (FISC) on the number of applications or certifications submitted to the court and whether those submissions were granted, modified, or denied. It also includes information relating to amicus curiae appointments by the Foreign Intelligence Surveillance Courts.

On June 2, 2015, Congress enacted the USA FREEDOM Act of 2015 (Pub. L. No. 114-23). One of the provisions of this Act, codified at 50 U.S.C. § 1873 (a) (2), which requires the Director of the Administrative Office of the U.S. Courts (AO) to publish the report on the AO's internet website.

The report is required to contain the following information (all section numbers refer to Title 50 of the U.S. Code):

1. the number of applications or certifications for orders submitted under each of sections 1805, 1824, 1842, 1861, 1881a, 1881b, and 1881c;
2. the number of such orders granted under each of those sections;
3. the number of orders modified under each of those sections;
4. the number of applications or certifications denied under each of those sections;
5. the number of appointments of an individual to serve as amicus curiae under section 1803, including the name of each individual appointed to serve as amicus curiae; and
6. the number of findings issued under section 1803(i) that such appointment is not appropriate.

Honorable Bob Goodlatte
Chairman
Committee on the Judiciary
United States House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

I herewith transmit the annual report for 2017 regarding the activities of the Foreign Intelligence Surveillance Courts as required in 50 U.S.C. § 1873. Enclosed is a copy of the version of the report that we are making available on an Internet Web site, pursuant to 50 U.S.C. § 1873(a)(2). We are separately providing to you a classified version of the report.

The report indicates that in calendar year 2017 the Foreign Intelligence Surveillance Court denied 26 applications in full and 50 applications in part. The Court modified the orders sought in an additional 391 applications and granted the orders sought without modifications for 1,147 applications. No amicus curiae were appointed during the reporting period and no findings were made under 50 U.S.C. § 1803(i)(2)(A). The report addresses three matters in which the Court advised the government that it was considering appointment of an amicus curiae.

The Executive Branch has conducted the declassification review specified in 50 U.S.C. § 1873(a)(1). The Department of Justice advised us that one figure in the report is classified at this time. We are not reporting this figure in the public version of the report, but we included it in the classified version separately provided to you.

Table 1

In accordance with the reporting requirements specified in 50 U.S.C. § 1873(a)(1), the statistics in this table are itemized by section of the Statute. Some of the statistics reported herein differ from those in comparable reports prepared by the U.S. Department of Justice (DOJ) and the Director of National Intelligence (DNI) because those agencies track and tabulate actions taken only with respect to final applications and certifications filed pursuant to Rule 9(b).

Section	Applications or Certifications	Orders Granted	Orders Modified	Orders Denied in Part	Applications or Certifications Denied
1805 only	104	60	36	4	4
1824 only	33	20	9	2	2
1805 and 1824[†]	1,235	868	308	41	18
1842	34	19	13	1	1
1861	118	92	23	2	1
1881a	0	0	[redacted][‡]	0	0
1881b	0	0	0	0	0
1881c	90	88	2	0	0

[†] Requests for combined authority to conduct electronic surveillance and physical searches under 50 U.S.C. § 1805 and § 1824, respectively, are included in this row and are not separately reflected in the rows addressing requests for authority to conduct electronic surveillance (Section 1805) and physical search (Section 1824) above.

[‡] This number reflects certification(s) submitted during calendar year 2016 that were decided in 2017. No additional certifications were submitted during 2017. After completing the declassification review specified in 50 U.S.C. § 1873(a)(1), the U.S. Department of Justice has advised the AO that this number is currently classified for national security reasons.

The National Security Division (NSD) was created in March 2006 by the USA PATRIOT Reauthorization and Improvement Act (Pub. L. No. 109-177). The creation of the NSD consolidated the Justice Department's primary national security operations: the former Office of Intelligence Policy and Review and the Counterterrorism and Counterintelligence and Export Control Sections of the Criminal Division. The new Office of Law and Policy and the Executive Office, as well as the Office of Justice for Victims of Overseas Terrorism (which previously operated out of the Criminal Division) complete the NSD. The NSD commenced operations in September 2006 upon the swearing in of the first Assistant Attorney General for National Security.

The mission of the National Security Division is to carry out the Department's highest priority: protect the United States from threats to our national security by pursuing justice through the law. The NSD's organizational structure is designed to ensure greater coordination and unity of purpose between prosecutors and law enforcement agencies, on the one hand, and intelligence attorneys and the Intelligence Community, on the other, thus strengthening the effectiveness of the federal government's national security efforts.

ASSISTANT ATTORNEY GENERAL JOHN C. DEMERS

Download image

John Demers became Assistant Attorney General for the National Security Division on February 22, 2018. As Assistant Attorney General, John oversees all units and components of the NSD, including the Counterterrorism Section, the Counterintelligence and Export Control Section, the Office of Intelligence, the Office of Law and Policy, the Foreign Investment Review Staff and the Office of Justice for the Victims of Overseas Terrorism. Prior to rejoining the Department of Justice, John was Vice President and Assistant General Counsel at The Boeing Company. He held several senior positions at the company including in Boeing Defense, Space, and Security and as lead lawyer and head of international government affairs for Boeing International.

From 2006 to 2009, John served on the first leadership team of the Justice Department's National Security Division, first as Senior Counsel to the Assistant Attorney General and then as Deputy Assistant Attorney General for the Office of Law & Policy. Before that, he served in the Office of Legal Counsel. From 2010-2017, he taught national security law as an adjunct professor at the Georgetown University Law Center. John worked in private practice in Boston and clerked for Associate Justice Antonin Scalia of the U.S. Supreme Court and Judge Diarmuid O'Scannlain of the U.S. Court of Appeals for the Ninth Circuit. He graduated from Harvard Law School and the College of the Holy Cross.

SUMMARY OF MAJOR U.S. EXPORT ENFORCEMENT, ECONOMIC ESPIONAGE, AND SANCTIONS-RELATED CRIMINAL CASES
(January 2015 to the present: updated January 19, 2018)

Below are brief descriptions of some of the major export enforcement and sanctions-related criminal prosecutions by the Department of Justice since January 2015. These cases resulted from investigations by Homeland Security Investigations (HSI), the Federal Bureau of Investigation (FBI), the Department of Commerce's Bureau of Industry and Security (BIS), the Pentagon's Defense Criminal Investigative Service (DCIS), and other law enforcement agencies. This list represents only select cases and is not exhaustive.

Microwave Integrated Circuits for China - On Jan. 19, 2018, in the Central District of California, Yi-Chi Shih, an electrical engineer who is a part-time Los Angeles resident, and Kiet Ahn Mai were arrested pursuant to a criminal complaint. The complaint alleges that Shih and Mai conspired to illegally provide Shih with unauthorized access to a protected computer of a United States company that manufactured specialized, high-speed computer chips known as monolithic microwave integrated circuits (MMICs). The conspiracy count also alleges that the two men engaged in mail fraud, wire fraud, and international money laundering to further the scheme. It also alleges that Shih violated the International Emergency Economic Powers Act (IEEPA). The complaint affidavit alleges that Shih and Mai executed a scheme to defraud the U.S. company out of its proprietary, export-controlled items, including technology associated with its design services for MMICs. The victim company's proprietary semiconductor technology has a number of commercial and military applications, and its customers include the Air Force, Navy, and the Defense Advanced Research Projects Agency. MMICs are used in electronic warfare, electronic warfare countermeasures, and radar applications. As part of the scheme, Shih and Mai accessed the victim company's computer systems via its web portal after Mai obtained that access by posing as a domestic customer seeking to obtain custom-designed MMICs that would be used solely in the United States. Shih and Mai allegedly concealed Shih's true intent to transfer the U.S. company's technology and products to the People's Republic of China, and specifically to Chengdu GaStone Technology Company (CGTC), a

SECTIONS & OFFICES

NSD Organization Chart

Counterterrorism Section

Counterintelligence and Export Control Section

Foreign Investment Review Staff

Office of Intelligence

- Operations Section
- Oversight Section
- Litigation Section

Office of Justice for Victims of Overseas Terrorism

Law and Policy Office

Executive Office

Counterterrorism Section

The Counterterrorism Section (CTS) is responsible for the design, implementation, and support of law enforcement efforts, legislative initiatives, policies and strategies relating to combating international and domestic terrorism. The Section seeks to assist, through investigation and prosecution, in preventing and disrupting acts of terrorism anywhere in the world that impact on significant United States interests and persons.

Learn More

Counterintelligence and Export Control Section

The Counterintelligence and Export Control Section (CES) supervises the investigation and prosecution of cases affecting national security, foreign relations, and the export of military and strategic commodities and technology. The Section has executive responsibility for authorizing the prosecution of cases under criminal statutes relating to espionage, sabotage, neutrality, and atomic energy. It provides legal advice to U.S. Attorney's Offices and investigative agencies on all matters within its area of responsibility, which includes 88 federal statutes affecting national security. It also coordinates criminal cases involving the application of the Classified Information Procedures Act. In addition, the Section administers and enforces the Foreign Agents Registration Act of 1938 and related disclosure statutes.

Related Topics:

- Foreign Agents Registration Act (FARA)
- Export Enforcement Case Fact Sheet

Foreign Investment Review Staff

The Foreign Investment Review Staff (FIRS) is responsible for three main portfolios of work. First, FIRS manages the Department of Justice's participation on the Committee on Foreign Investment in the United States (CFIUS), an inter-agency body statutorily required to review certain transactions that could result in control of a U.S. business by a foreign person, in order to determine the effect of such acquisitions on the national security of the United States. Second, FIRS leads the Department's efforts on Team Telecom, an informal inter-agency working group that considers the law enforcement, national security, and public safety implications of applications for licenses from the Federal Communications Commission involving a threshold percentage of foreign ownership or control. Third, FIRS monitors compliance with agreements or orders that mitigate concerns arising from prior CFIUS or Team Telecom cases.

Office of Intelligence

The Department of Justice has played a critical role in the nation's effort to prevent acts of terrorism and to thwart hostile foreign intelligence activities. Since the 9/11 terrorist attacks, the National Security Division's (NSD) Office of Intelligence (successor to the Office of Intelligence Policy and Review (OIPR)) has grown dramatically in an effort to ensure: that Intelligence Community agencies have the legal authorities necessary to conduct intelligence operations, particularly operations involving the Foreign Intelligence Surveillance Act (FISA); that the office exercises meaningful oversight over various national security activities of Intelligence Community agencies; and that it can play an effective role in FISA-related litigation.

Learn More

Operations Section

The Operations Section handles NSD's intelligence operations workload, including representing the government before the Foreign Intelligence Surveillance Court (FISC). The Operations Section is responsible for preparing and filing all applications for Court orders pursuant to FISA. The mission of the section is to ensure that the FBI and other Intelligence Community agencies have the legal tools necessary to conduct intelligence operations in adherence to the requirements and safeguards of the law. The Operations Section is divided into three operational units: the Counterterrorism Unit, the Counterintelligence Unit, and the Special Operations Unit. In addition to its legal staff, the Operations Section is supported by two intelligence research specialists and employees who work as part of the Classified Information Management Unit.

The Operations Section also works with the Oversight Section in various matters, including overseeing compliance with FISC orders and working on projects involving information sharing among Intelligence Community agencies and modifications to authorities governing the acquisition, retention, and dissemination of FISA-related information. In addition, the Operations Section closely coordinates with the FBI and other Intelligence Community agencies on intelligence operational matters and provides legal advice to other government agencies on matters relating to FISA and other national security laws and governing authorities.

Oversight Section

The Department of Justice bears the responsibility of overseeing the foreign intelligence, counterintelligence and other national security activities of the United States Intelligence Community to ensure compliance with the Constitution, statutes and Executive Branch policies. In fulfilling this responsibility, the Department must weigh the need to protect individual privacy and civil liberties against the need of the United States to gather foreign intelligence. The Oversight Section of the National Security Division's Office of Intelligence is

U.S. Department of Justice
National Security Division

Washington, D.C. 20530

October 2, 2016

GUIDANCE REGARDING VOLUNTARY SELF-DISCLOSURES, COOPERATION, AND REMEDIATION IN EXPORT CONTROL AND SANCTIONS INVESTIGATIONS INVOLVING BUSINESS ORGANIZATIONS[1]

Introduction

Foreign governments and other non-state adversaries of the United States are engaged in an aggressive campaign to acquire superior technologies and commodities that are developed, manufactured, and controlled in, and by, the United States. Such acquisitions – when conducted in contravention of U.S. law and policy – undermine the comparative and competitive advantages of U.S. industries and warfighters and, consequently, the national and economic security of the United States.

Thwarting these unlawful efforts is a top priority for the National Security Division (NSD) of the Department of Justice (DOJ). Working in partnership with U.S. Attorneys'

COMBATTING NATIONAL SECURITY CYBER THREATS

Cyber-based threats to the national security are the biggest emerging threats we face, and they present some of our biggest challenges here and now. Building on the creation of the National Security Cyber Specialist (NSCS) network – which was created with the goal to get ahead of the threat – NSD will continue to enhance its focus on cyber threats to the national security.

Michigan Residents Arrested for Conspiracy to Provide Material Support to ISIS

Three residents of Lansing, Michigan, were arrested without incident Monday afternoon for conspiring to provide material support to a designated foreign terrorist organization, namely the Islamic State of Iraq and al-Sham (ISIS). The U.S. Attorney's Office for the Western District of Michigan charged all three in a criminal complaint filed today in U.S. District Court in Grand Rapids, Michigan. The conspiracy charge is punishable by up to 20 years in federal prison.

Members of the FBI Joint Terrorism Task Force (JTTF) arrested Muse Abdikadir Muse (Muse Muse) at the Gerald R. Ford Airport in Grand Rapids, Michigan, after checking in for a flight to the first of a series of destinations on his way to Mogadishu, Somalia. Shortly thereafter, law enforcement arrested alleged coconspirators Mohamud Abdikadir Muse (Mohamud Muse), and Mohamed Salat Haji (Haji). All three defendants are naturalized U.S. citizens who were born in Kenya.

According to the complaint affidavit, Muse Muse purchased airline tickets earlier this month to travel from Grand Rapids to Mogadishu, departing on Monday, January 21, 2019. Among other support, the complaint alleged Haji and Mohamud Muse aided in the purchase of the ticket and drove Muse Muse to the Grand Rapids airport, each knowing the true purpose of the travel was for Muse Muse to join and fight for ISIS.

The complaint asserts that all three defendants pledged allegiance to ISIS through videos they recorded themselves. Muse Muse and Haji allegedly discussed with each other their desire to join ISIS, to kill non-believers, and even to potentially use a car for a martyrdom operation to run down non-believers here in the United States if they could not travel overseas to fight for ISIS. Following the arrests, federal agents executed search warrants at a residence shared by Mohamud Muse and Muse Muse.

Assistant Attorney General for National Security John C. Demers, Andrew B. Birge, U.S. Attorney for the Western District of Michigan, and Tim Slater, Special Agent in Charge, Federal Bureau of Investigation, Detroit Field Division, announced the arrests.

The public is reminded that a complaint contains only charges and is not evidence of guilt. A defendant is presumed innocent and is entitled to a fair trial at which the government has the burden of proving guilt beyond a reasonable doubt.

Attachment(s):
Download Criminal Complaint
Download Criminal Complaint Continuation Sheet

Press Release Number:
19-8

This criminal complaint is based on these facts:

☑ Continued on the attached sheet.

Sworn over the telephone and recorded

~~Sworn to before me and signed in my presence.~~

Date: 11:24 AM, Jan 21, 2019

City and state: Grand Rapids, Michigan

Complainant's signature

Peter Jolliffe, Special Agent FBI

Printed name and title

Judge's signature

Phillip J. Green, U.S. Magistrate Judge

Printed name and title

CONTINUATION SHEET FOR CRIMINAL COMPLAINT

I, Peter C. Jolliffe, being first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of a Complaint charging **MOHAMUD ABDIKADIR MUSE (MUSE)**; his brother, **MUSE ABDIKADIR MUSE (MM)**; and their brother-in-law/cousin, **MOHAMED SALAT HAJI (HAJI)**; with conspiring to provide material support or resources to a designated foreign terrorist organization; to wit: ISIS - in violation of 18 U.S.C. § 2339B, between in or about October 30, 2018 and on or about January 21, 2019, in the Western District of Michigan and elsewhere.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been employed as a federal investigator for nine years. As a Special Agent with the FBI, my duties include the investigation of alleged violations of federal criminal laws, including terrorism offenses.

3. The information contained in this affidavit comes from my personal observations, my training and experience, and information provided to me by other law enforcement officers who have participated in this investigation. This affidavit is intended to articulate sufficient probable cause to support charges in the

8. MUSE is a 23-year-old male, who was born in Kenya and is a derivative U.S. citizen. MM is a 20-year-old male and the younger brother of MUSE; he too was born in Kenya and is a derivative U.S. citizen. HAJI is a 26-year-old male and is the brother-in-law of MUSE and MM. He was also born in Kenya and is a naturalized U.S. citizen. MUSE, MM and HAJI all reside in Lansing, MI, within the Western District of Michigan.

9. In or about April of 2016, Facebook account "Mohamud A Musa" (FB Account-Muse #1) came to the attention of the FBI based on material that was posted on the account's publicly viewable pages. The initial FBI review of FB Account-Muse # 1 revealed frequent posts of photos, videos, and statements and commentary that were pro-ISIS in nature and what can be described as violent, extremist propaganda. In or about the Fall of 2016, FBI analysis of certain photos posted to FB Account-Muse #1 led to former Omaha, Nebraska resident MUSE. In August 2016, MUSE was issued a Michigan driver's license reflecting a Lansing, Michigan address. MUSE's Facebook verified phone number contains an account birth date that links to MUSE's actual birth date.

33. On or about December 18, 2018, MM, via FB Account-MM #2 sent a link of available flights from Chicago, Illinois to Mogadishu, Somalia to UCE-3. MM wrote, "It could be very soon that we are in Somalia" and "the other two whi should be coming with me [MM] have family that they need to make sure are safe so there being little more cautious with there steps, me I'm just ready to leave as soon as I get that passport."

34. On or about December 20-21, 2018, the following was exchanged between UCE-3 and FB Account-MM #2: MM stated to UCE-3 that his passport should arrive next week. MM stated that if he and UCE-3 both receive their passports before January 21, 2019, that he and UCE-3 can leave before then. MM requested help from UCE-3 searching for a flight and told UCE-3 to look for a route from Turkey to Djibouti to Mogadishu. MM and UCE-3 exchanged communications about cheaper flights originating from Grand Rapids Airport with a route consisting of Orlando, Stockholm, Dubai, Hargesia to Mogadishu, at a cost of approximately $1,799 per person. MM stated that as long as he and UCE-3 "arrive in Mogadishu, it's cool." MM told UCE-3 that when the passports arrive and tickets are purchased, that these will be the "proof of sincerity" to the mujahedeen. MM stated he had $500 to contribute toward the airline ticket cost.

OFFICE OF PRIVACY & CIVIL LIBERTIES

OFFICE OF PRIVACY AND CIVIL LIBERTIES

LEADERSHIP

Peter A. Winn
Acting Chief Privacy and Civil Liberties Officer

Kathy Harman-Stokes
Deputy Director, Office of Privacy and Civil Liberties

CONTACT

Office of Privacy and Civil Liberties
privacy@usdoj.gov

- Reviews, oversees, and coordinates DOJ privacy operations.
- Ensures DOD compliance with 1974 Privacy Act, 2002 E-Government Act, 2014 Federal Information Security Modernization Act (FISMA), and 2015 Judicial Redress Act.
- Develops departmental privacy training.
- Prepares privacy-related reporting to the President & Congress.
- Reviews DOJ information-handling practices to ensure consistency with protecting privacy and civil liberties.

PURDUE UNIVERSITY
Libraries

OVERVIEW OF THE PRIVACY ACT OF 1974

(2015 Edition)

TABLE OF CONTENTS

Department of Justice Policy Guidance[1]

Domestic Use of Unmanned Aircraft Systems (UAS)

INTRODUCTION

The law enforcement agencies of the Department of Justice ("the Department") work diligently to protect the American people from national security threats, enforce our nation's laws, and ensure public safety. In doing so, these agencies use a wide variety of investigative methods. Some of these methods have been in use for decades; others are relatively new and rely on technological innovation. In all cases, investigations and other activities must be conducted consistent with the Constitution and the laws of the United States—and with our commitment to protecting privacy and civil liberties.

In recent years, Unmanned Aircraft Systems (UAS)[2] have emerged as a viable law enforcement tool. UAS have been used to support kidnapping investigations, search and rescue operations, drug interdictions, and fugitive investigations. While they are, in many ways, similar to the manned aircraft that have been in use for many years, they have the potential to provide law enforcement with additional flexibility and yield life-saving benefits. UAS also have the

RESPECT FOR CIVIL RIGHTS AND CIVIL LIBERTIES

Respect for civil rights and civil liberties is a core tenet of our democracy. In executing the Department's law enforcement and national security missions, personnel must rigorously support and defend the Constitution and continue to uphold the laws, regulations and policies that govern our activities and operations.

As with all investigative methods, UAS must be operated consistent with the U.S. Constitution. The Fourth Amendment protects individuals from unreasonable searches and seizures and generally requires law enforcement to seek a warrant in circumstances in which a person has a reasonable expectation of privacy. Moreover, Department personnel may never use UAS solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution and laws of the United States. Department personnel may never use UAS to engage in discrimination that runs counter to the Department's policies on race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity. Department personnel must also be trained to understand and abide by all relevant federal legal standards applicable to the use of UAS, and to seek advice from legal counsel as necessary.

In addition, UAS may only be used in connection with properly authorized investigations and activities. Statutory authorities, the Attorney General's Guidelines, and other relevant agency policies and guidance define the scope of authorized investigations and activities and require regular supervisory review and approval. UAS must continue to be used within the context of these existing safeguards.

PRIVACY AND CIVIL LIBERTIES ACTIVITIES SEMI-ANNUAL REPORT

SECOND SEMI-ANNUAL REPORT, FY 2016

APRIL 1, 2016 – SEPTEMBER 30, 2016

CONGRESSIONAL INTELLIGENCE COMMITTEES

- U.S. Govt. has used contingency secret service funding for intelligence operations since George Washington Administration.
- After 1947 CIA Establishment, congressional oversight assigned to House & Senate Armed Services Committees and House & Senate Appropriations Committee Defense Subcommittees. Joint Intelligence Committee proposed in 1948 and after.
- Actual awareness of CIA and intelligence agencies activities limited to committee and subcommittee chairs and ranking members.
- Congressional staff awareness limited to one or two senior staff members of these committees/subcommittees who worked to ensure intelligence agency needs were included in DOD budget.
- Periodic reform proposals made but didn't go anywhere.
- Increasing public disenchantment with Vietnam War, Watergate, and media revelation controversial intelligence agency actions, such as covert operations, brought about pressure for reform and enhanced congressional oversight.
- Senate Select Intelligence Committee established May 19, 1976.
- House Select Intelligence Committee established July 14, 1977.

HOUSE INTELLIGENCE COMMITTEE
CHAIR REP. ADAM SCHIFF (D-CA) RANKING MEMBER REP. DEVIN NUNES (R-CA)

- Subcommittees:
- CIA Subcommittee
- Dept. of Defense Intelligence and Overhead Architecture Subcommittee
- Emerging Threats Subcommittee
- NSA and Cybersecurity Subcommittee

Highlights of H.R. 6237

The Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018 and 2019

On June 27, 2018, Chairman Nunes introduced H.R. 6237, The Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018 and 2019. By unanimous vote, the House Permanent Select Committee on Intelligence reported H.R. 6237 out of Committee on June 28, 2018.

This legislation provides the Intelligence Community (IC) the necessary resources and authorities to ensure the IC remains capable of protecting and defending the United States. The bill supports critical national security programs, particularly those focused on countering threats from China as well as cyberattacks; the legislation does not make any changes to key surveillance authorities. The total funding levels authorized by the bill are slightly above the President's budget, balancing fiscal discipline and national security. This legislation:

- **Improves Retention and Recruitment of Personnel for Critical Cyber Missions** by providing increased pay for certain employees with unique cyber skills;
- **Defends Against Foreign Threats to Elections** by requiring the Director of National Intelligence to electronically publish an unclassified advisory report on foreign counterintelligence and cybersecurity threats to election campaigns for federal offices;
- **Protects Key Energy Infrastructure** by creating an Infrastructure Security Center within the Department of Energy to coordinate intelligence on significant threats;

The Honorable Michael Mulvaney
Acting Chief of Staff
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20006

The Honorable Dan Coats
Director of National Intelligence
Office of the Director of National Intelligence
Washington, D.C. 20511

The Honorable David J. Glawe
Under Secretary for Intelligence & Analysis
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Mr. Mulvaney, Director Coats, and Under Secretary Glawe:

I write to raise two concerns about the Administration's use of intelligence and other information in formulating policy and making public statements in recent months about the U.S southern border.

The first involves the basis for the Administration's inflammatory claims about threats to national security. In recent days, President Trump and Administration officials have charged that our border with Mexico is host to a "growing humanitarian and security crisis."[1] That claim stems in part from the Administration's assertion of a purported terrorist threat to the U.S. homeland at the southern border. For example, the Administration has cited the statistic that DHS prevented 3,755 known or suspected terrorists (KSTs) from entering the country in fiscal

115TH CONGRESS
2d Session

HOUSE OF REPRESENTATIVES

REPORT
115–1111

REPORT ON THE ACTIVITY

OF THE

HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

FOR THE

ONE HUNDRED AND FIFTEENTH CONGRESS

CONTENTS

JURISDICTION AND SPECIAL OVERSIGHT FUNCTION

Clause 11(b)(1) of rule X of the Rules of the House of Representatives for the 115th Congress sets forth the jurisdiction of the Permanent Select Committee on Intelligence—

(A) The Central Intelligence Agency, the Director of National Intelligence, and the National Intelligence Program as defined in section 3(6) of the National Security Act of 1947.

(B) Intelligence and intelligence-related activities of all other departments and agencies of the Government, including the tactical intelligence and intelligence-related activities of the Department of Defense.

(C) The organization or reorganization of a department or agency of the Government to the extent that the organization or reorganization relates to a function or activity involving intelligence or intelligence-related activities.

(D) Authorizations for appropriations, both direct and indirect, for the following:

(i) The Central Intelligence Agency, the Director of National Intelligence, and the National Intelligence Program as defined in section 3(6) of the National Security Act of 1947.

(ii) Intelligence and intelligence-related activities of all other departments and agencies of the Government, in-

LEGISLATIVE AND OVERSIGHT ACTIVITIES

During the 115th Congress, 91 bills or resolutions were referred to the Permanent Select Committee on Intelligence (the Committee).

Committee Action

The Committee reported three measures to the House. Those measures were: H.R. 3180, the Intelligence Authorization Act for Fiscal Year 2018, introduced by Chairman Devin Nunes; H.R. 4478, the FISA Amendments Reauthorization Act of 2017, introduced by Chairman Devin Nunes; and H.R. 6237, the Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018 and 2019, introduced by Chairman Devin Nunes.

The Committee discharged one additional measure: H.R. 5925, the Coordinated Response through Interagency Strategy and Information Sharing Act, introduced by Mr. Trey Gowdy, a member of the Committee.

Other Measures Within the Committee's Jurisdiction

In addition to those measures described above, four measures referred to the Committee passed the House. Those measures were: H.R. 3030, Elie Wiesel Genocide and Atrocities Prevention Act of 2018, introduced by Mrs. Ann Wager; H.R. 3364, the Countering America's Adversaries Through Sanctions Act, introduced by Mr. Edward Royce; H.R. 5841, the Foreign Investment Risk Review Modernization Act of 2018, introduced by Mr. Robert Pittenger; and H. Res. 970, Insisting that the Department of Justice fully comply with the requests, including subpoenas, of the Permanent Select Committee on Intelligence and the subpoena issued by the Committee on the Judiciary relating to potential violations of the Foreign Intelligence Surveillance Act by personnel of the Department of Justice and related matters, introduced by Mr. Mark Meadows.

On April 10, 2018, the Committee held a closed briefing.
On April 12, 2018, the Department of Defense Intelligence Overhead Architecture Subcommittee held a closed hearing.
On April 16, 2018, the Committee held a closed roundtable.
On April 24, 2018, the Committee held a closed briefing.
On April 26, 2018, the Central Intelligence Agency Subcommittee held a closed hearing.
On May 7, 2018, the Committee held a closed briefing.
On May 10, 2018, the Committee held a closed briefing.
On May 15, 2018, the Committee held a closed briefing.
On May 17, 2018, the Committee held an open hearing.
On May 21, 2018, the Committee held a closed briefing.
On May 22, 2018, the Central Intelligence Agency Subcommittee held a closed hearing.
On May 24, 2018, the Central Intelligence Agency Subcommittee held a closed briefing.
On June 5, 2018, the Committee held a closed briefing.
On June 12, 2018, the Committee held a closed briefing.
On June 14, 2018, the Department of Defense Intelligence Overhead Architecture Subcommittee held a closed briefing.
On June 21, 2018, the Committee held a closed hearing.
On June 25, 2018, the Committee held a closed briefing.
On June 28, 2018, the Committee held a closed business meeting.
On July 10, 2018, the Committee held a closed briefing.
On July 16, 2018, the Committee held a closed briefing.
On July 19, 2018, the Committee held an open hearing.
On July 23, 2018, the Committee held a closed briefing.
On July 24, 2018, the Committee held a closed roundtable.
On July 26, 2018, the Central Intelligence Agency and NSA & Cybersecurity Subcommittees held a closed joint briefing.
On September 4, 2018, the Committee held a closed briefing.
On September 12, 2018, the Committee held a closed roundtable.
On September 25, 2018, the Committee held a closed briefing.

U.S. Senate Select Committee on

Intelligence

Committee Members

Richard Burr
North Carolina
Chairman

Mark Warner
Virginia
Vice Chairman

Republicans

James Risch - Idaho
Marco Rubio - Florida
Susan Collins - Maine
Roy Blunt - Missouri
Tom Cotton - Arkansas
John Cornyn - Texas
Ben Sasse - Nebraska

Democrats

Dianne Feinstein - California
Ron Wyden - Oregon
Martin Heinrich - New Mexico
Angus King - Maine
Kamala Harris - California
Michael Bennet - Colorado

DIVISION N--INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2017

SEC. 1. SHORT TITLE; TABLE OF CONTENTS.

(a) Short Title.--This division may be cited as the ``Intelligence Authorization Act for Fiscal Year 2017".

(b) Table of Contents.--The table of contents for this division is as follows:

"SEC. 113B. SPECIAL PAY AUTHORITY FOR SCIENCE, TECHNOLOGY, ENGINEERING, OR MATHEMATICS POSITIONS.

"(a) AUTHORITY TO SET SPECIAL RATES OF PAY.—Notwithstanding part III of title 5, United States Code, the head of each element of the intelligence community may establish higher minimum rates of pay for 1 or more categories of positions in such element that require expertise in science, technology, engineering, or mathematics (STEM).

"(b) MAXIMUM SPECIAL RATE OF PAY.—A minimum rate of pay established for a category of positions under subsection (a) may not exceed the maximum rate of basic pay (excluding any locality-based comparability payment under section 5304 of title 5, United States Code, or similar provision of law) for the position in that category of positions without the authority of subsection (a) by more than 30 percent, and no rate may be established under this section in excess of the rate of basic pay payable for level IV of the Executive Schedule under section 5315 of title 5, United States Code.

"(c) NOTIFICATION OF REMOVAL FROM SPECIAL RATE OF PAY.—If the head of an element of the intelligence community removes a category of positions from coverage under a rate of pay authorized by subsection (a) after that rate of pay takes effect—

"(1) the head of such element shall provide notice of the loss of coverage of the special rate of pay to each individual in such category; and

"(2) the loss of coverage will take effect on the first day of the first pay period after the date of the notice.

Hearing Type: Open
Date & Time: Wednesday, May 9, 2018 - 9:30am
Location: Hart 216

Witnesses

Deputy Director Gina Haspel
CIA

- Opening Statement
- Response to Questionnaire for Completion by Presidential Nominees
- Response to Committee Additional Pre-Hearing Questions
- Response to Committee Post-Hearing Questions

Full Transcript

View Full Transcript

Hearings

Hearing Type: Open
Date & Time: Tuesday, January 29, 2019 - 9:30am
Location: Hart 216

Witnesses

Director Christopher Wray
Federal Bureau of Investigation
FBI

Director Gina Haspel
Central Intelligence Agency
CIA

Director Daniel Coats
Office of the Director of National Intelligence
ODNI

Director General Robert Ashley
Defense Intelligence Agency
DIA

Director General Paul Nakasone
National Security Agency
NSA

Director Robert Cardillo
National Geospatial-Intelligence Agency
NGA

STATEMENT FOR THE RECORD

WORLDWIDE THREAT ASSESSMENT

OF THE US INTELLIGENCE COMMUNITY

Daniel R. Coats
Director of National Intelligence

Senate Select Committee on Intelligence

29 JANUARY 2019

ONLINE INFLUENCE OPERATIONS AND ELECTION INTERFERENCE

Our adversaries and strategic competitors probably already are looking to the 2020 US elections as an opportunity to advance their interests. More broadly, US adversaries and strategic competitors almost certainly will use online influence operations to try to weaken democratic institutions, undermine US alliances and partnerships, and shape policy outcomes in the United States and elsewhere. We expect our adversaries and strategic competitors to refine their capabilities and add new tactics as they learn from each other's experiences, suggesting the threat landscape could look very different in 2020 and future elections.

- Russia's social media efforts will continue to focus on aggravating social and racial tensions, undermining trust in authorities, and criticizing perceived anti-Russia politicians. Moscow may employ additional influence toolkits—such as spreading disinformation, conducting hack-and-leak operations, or manipulating data—in a more targeted fashion to influence US policy, actions, and elections.

- Beijing already controls the information environment inside China, and it is expanding its ability to shape information and discourse relating to China abroad, especially on issues that Beijing views as core to party legitimacy, such as Taiwan, Tibet, and human rights. China will continue to use legal, political, and economic levers—such as the lure of Chinese markets —to shape the information environment. It is also capable of using cyber attacks against systems in the United States to censor or suppress viewpoints it deems politically sensitive.

- Iran, which has used social media campaigns to target audiences in both the United States and allied nations with messages aligned with Iranian interests, will continue to use online influence operations to try to advance its interests.

INTELLIGENCE LEGAL REFERENCE BOOK 2016

TABLE OF CONTENTS

PURDUE UNIVERSITY
Libraries

(e) "COVERT ACTION" DEFINED. —As used in this title, the term "covert action" means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include—

(1) activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;

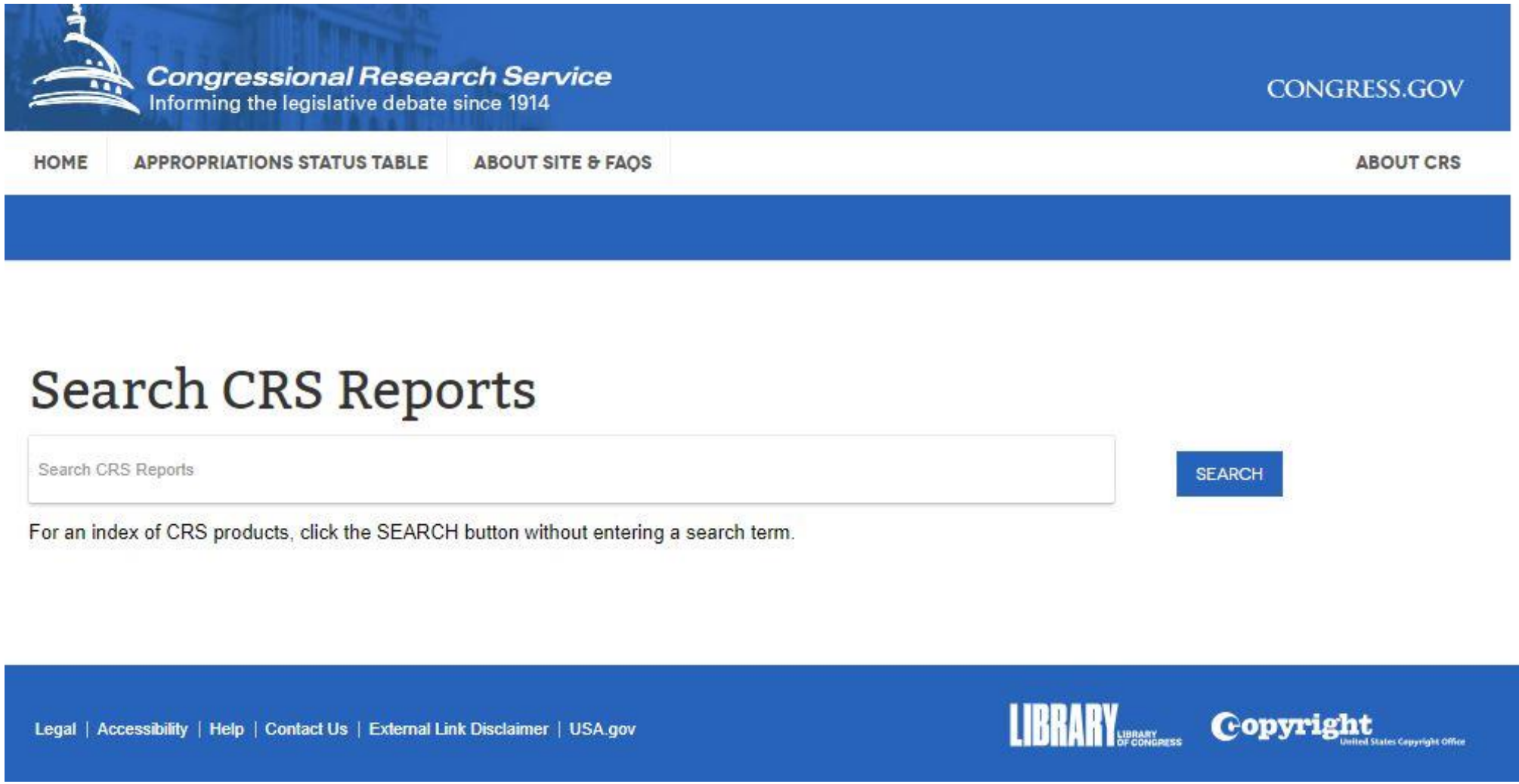
(2) traditional diplomatic or military activities or routine support to such activities;

(3) traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or

(4) activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2), or (3)) of other United States Government agencies abroad.

(f) PROHIBITION ON CONVERT ACTIONS INTENDED TO INFLUENCE UNITED STATES POLITICAL PROCESSES, ETC. —No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media.

CONGRESSIONAL RESEARCH SERVICE (CRS)



PURDUE UNIVERSITY
Libraries

Congressional Research Service

Informing the legislative debate since 1914

Covert Action and Clandestine Activities of the Intelligence Community: Framework for Congressional Oversight In Brief

Updated May 15, 2018

Contents

Risk Assessment

"The executive branch is chiefly concerned with achieving the objectives of the president, whatever they might be. Because of this, it is sometimes tempted to downplay the risk and accentuate the gain."[23] Congress's relative distance from conceiving and planning the activity may enable it to provide more dispassionate risk assessment and more accurate analysis of likely outcomes.

Questions for Congress

- Does the covert action involve an unacceptable risk of escalating into a broader conflict or war?
- In the event of an unauthorized or untimely disclosure—or a popular perception of U.S. involvement—what are the risks to U.S. national security, U.S. personnel, or relations with states in the region?
- What are the consequences of failure of the covert action or clandestine intelligence activity to U.S. lives, U.S. national security, and relations with states in the region?
- If U.S. Armed Forces are involved, is the covert action or clandestine activity being conducted such that U.S. Armed Forces retain full protection under the terms of the Geneva Conventions?
- Is it plausible for the U.S. role to remain secret and deniable? Or is there substantial or unacceptable risk of compromising U.S. sponsorship, to the

Congressional Research Service

Informing the legislative debate since 1914

Congressional Oversight of Intelligence: Background and Selected Options for Further Reform

Background and Selected Options for Further Reform

Michael E. DeVine
Analyst in Intelligence and National Security

Prior to the establishment of the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI) in 1976 and 1977, respectively, Congress did not take much interest in conducting oversight of the intelligence community (IC). The Subcommittees on the Central Intelligence Agency (CIA) of the congressional Armed Services Committees had nominal oversight responsibility, though Congress generally trusted that IC could more or less regulate itself and conduct activities that complied with the law, were ethical, and shared a common understanding of national security priorities. Media reports in the 1970s of the CIA's domestic surveillance of Americans opposed to the war in Vietnam, in addition to the agency's activities relating to national elections in Chile, prompted Congress to change its approach. In 1975, Congress established two select committees to investigate intelligence activities, chaired by Senator Frank Church in the Senate (the "Church Committee"), and Representative Otis Pike in the House (the "Pike Committee").

Following their creation, the Church and Pike committees' hearings revealed the possible extent of the abuse of authority by the IC and the potential need for permanent committee oversight focused solely on the IC and intelligence activities. SSCI and HPSCI oversight contributed substantially to Congress's work to legislate improvements to intelligence organization, programs, and processes, and it enabled a more structured, routine relationship with intelligence agencies. On occasion, this has resulted in Congress advocating on behalf of intelligence reform legislation that many agree has generally improved IC organization and performance. At other times, congressional oversight has been perceived as less helpful, delving into the details of programs and activities.

Selected Options for Further Reform

Following is an examination of selected oversight reform proposals that could be considered in developing a framework for discussion. The 9/11 Commission recommended most of them in its report, though some, such as the idea to establish a Joint Committee on Intelligence, have a much longer history.

Establish a Joint Committee for Intelligence

The 9/11 Commission recommended the establishment of a joint intelligence committee using the Joint Committee on Atomic Energy (JCAE) as a model.[32] The Joint Committee on Atomic Energy (JCAE) was established by the Atomic Energy Act of 1946 (P.L. 585, 60 Stat. 772-773). It had equal representation from the House and Senate. It was seen as largely bipartisan, fostered expertise among its members, influenced policy of the executive branch, and enabled more efficient oversight of matters under its jurisdiction. Unlike any other joint committee of Congress, the JCAE also had the authority to report legislation to the floor of the House and Senate. Until its termination in 1977, it had been considered by many to be one of the most powerful committees in Congress. It was terminated, however, in part due to its having developed what was perceived as a conflict of interest as both a committee that could influence policy on atomic energy uses and the oversight body for the Atomic Energy Commission.

The idea of a joint committee for oversight of intelligence was first proposed by the U.S. Commission on the Organization of the Executive Branch of the Government (the *Second Hoover*

BENEFITS OF STUDYING JUSTICE DEPT. AND CONGRESSIONAL COMMITTEE INTELLIGENCE INFORMATION RESOURCES

Understanding the Justice Dept's role in U.S. historic, current, and emerging intelligence activities and operations.

Understanding the role of the Foreign Intelligence Surveillance Court and Foreign Intelligence Surveillance Act (FISA)

Gaining enhanced awareness of the continuing balancing act between national security and civil liberties.

Gaining enhanced awareness of the importance of cybersecurity in intelligence operations and personal privacy and the importance of economic espionage.

Learning about the roles played by congressional intelligence oversight committees in intelligence agency operations.

Understanding the legal infrastructure behind U.S. intelligence agencies

Questions?

PURDUE UNIVERSITY
Libraries