



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

November 17, 2011

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

Dear Mr. Chairman:

Enclosed please find responses to questions for the record arising from the appearance of Gordon M. Snow, Assistant Director of the Cyber Division at the Federal Bureau of Investigation, at a hearing before the Committee on April 12, 2011, entitled "Cyber Security: Responding to the Threat of Cyber Crime and Terrorism." We apologize for the delay and hope this information is of assistance to the Committee.

Please do not hesitate to contact this office if we may provide additional assistance regarding this, or any other matter. The Office of Management and Budget has advised us that from the perspective of the Administration's program there is no objection to submission of this letter.

Sincerely,

A handwritten signature in dark ink, appearing to read "R. Weich".

Ronald Weich
Assistant Attorney General

Enclosure

cc: The Honorable Charles Grassley
Ranking Minority Member

**Responses of the Federal Bureau of Investigation
to Questions for the Record
Arising from the April 12, 2011, Hearing Before the
Senate Committee on the Judiciary
Regarding Cyber Security: Responding to the
Threat of Cyber Crime and Terrorism**

Questions Posed by Senator Feinstein

1. In your testimony, you note that in 2010, FBI arrested a record 202 individuals for [cyber] criminal intrusions, up from 159 in 2009. You also testified that on the criminal side a majority of the attacks come from individuals located in Russia and Eastern European countries. Can you provide, for each of the last five years:

a. The number of arrests for cyber crime offenses of individuals located in Russia?

Response:

<u>Year</u>	<u>Number of Arrests</u>
2006	3
2007	0
2008	1
2009	1
2010	2

These responses are current as of 6/14/11

b. The number of individuals located in Russia prosecuted for cyber crime offenses?

Response:

<u>Year</u>	<u>Number of Prosecutions</u>
2006	0
2007	3
2008	0
2009	1
2010	1

c. The number of arrests for cyber crime offenses of individuals located in Eastern Europe?

Response:

<u>Year</u>	<u>Number of Arrests</u>
2006	38
2007	37
2008	109
2009	81
2010	149

d. The number of individuals located in Eastern Europe prosecuted for cyber crime offenses?

Response:

<u>Year</u>	<u>Number of Prosecutions</u>
2006	0
2007	0
2008	9
2009	25
2010	16

These responses are current as of 6/14/11

Question Posed by Senator Whitehouse

2. Per my request at the hearing, please describe the extent to which your organization's cyber security resources are empowered to supplement criminal enforcement efforts with the use of civil injunctive tools to combat cyber security threats.

Response:

The FBI has recently begun using civil injunctions to combat cyber threats. Historically, the FBI has used solely criminal tools, which have been only partially effective because there are gaps in the forfeiture authorities available to address cybercrime; forfeiture and seizure tools provide limited functionality in this context; and subjects are often able to respond rapidly to our law enforcement efforts and avoid criminal consequences. While we continue to work to address the gaps in forfeiture authority for these crimes, the FBI's efforts to combat complex cyber crimes now benefit from the added flexibility afforded by civil tools. For example, temporary restraining orders and injunctions allow the FBI temporarily to operate computer servers involved in criminal cyber fraud, permitting us to disrupt and dismantle cyber security threats while preventing further victimization.

The recent investigation of the Coreflood botnet in Connecticut is an example of the benefits of supplementing criminal enforcement efforts with civil injunctions. In this instance, the FBI obtained multiple criminal seizure warrants, authorizing us to deactivate the existing Coreflood command and control servers. Simultaneously, we obtained a temporary restraining order that directed the defendants to stop engaging in fraud. The order also authorized the U.S. Marshals Service to respond to infected computers with "stop" commands and to use a substitute command and control server. This approach allowed the FBI to identify many of the victims and notify them of the fraudulent activity and their roles in the scheme. While the botnet was held static, anti-virus vendors were able to develop solutions for detecting and removing the Coreflood virus before a new variant could be released. When the substitute server was activated, it recorded approximately 2.4 million beacons from infected computers; after taking remediation action, the beacons received by the substitute command and control server indicated that the size of the Coreflood botnet had been reduced by approximately 80% domestically and 45% internationally. The temporary restraining order also allowed the FBI to work with private industry and our

These responses are current as of 6/14/11

foreign law enforcement partners to dismantle the Coreflood botnet. This was significantly preferable to using only criminal remedies, which would have allowed us only to seize the Coreflood command and control servers without addressing the underlying compromised computers. Those compromised computers could then have been recaptured by the subjects of the investigation.

Questions Posed by Senator Klobuchar

3. How does the FBI currently work with private sector entities to counter potential cyber threats before they emerge?

Response:

The FBI has developed strong relationships with private industry, establishing highly effective public-private partnerships such as InfraGard. Through InfraGard, state, local, and tribal law enforcement, academia, other government agencies, communities, and private industry work with us through our field offices to ward off attacks against critical infrastructure. Over the past 15 years, this initiative has grown to include more than 42,000 members in 86 chapters across the United States. The exchange of knowledge, experience, and resources generated by InfraGard is invaluable and contributes directly to our ability to counter potential cyber threats.

The FBI also partners directly with the Internet Crime Complaint Center (IC3) and the National Cyber Forensics and Training Alliance (NCFTA). Established in 2000, the IC3 is a partnership between the FBI and the National White Collar Crime Center that serves as a vehicle to receive, develop, and refer criminal complaints regarding cyber crime. Since it began, the IC3 has processed more than 2 million complaints. The NCFTA, which includes representatives of industry, academia, and the FBI, participates in cyber-forensic analysis, tactical response development, technology vulnerability analysis, and the development of advanced training. Both of these partnerships are critical in countering potential cyber threats to the nation's infrastructure, and the FBI routinely provides appropriate information to its InfraGard and NCFTA partners.

In addition to partnerships that address a broad range of cyber threats, the FBI also works directly with organizations that target specific types of cyber threats. For example, in order to better protect banks and consumers against online financial fraud, the FBI has partnered with the Financial Services Information

These responses are current as of 6/14/11

Sharing and Analysis Center (FS-ISAC) to develop a new model for intelligence-driven collaboration between law enforcement and the private sector. This working relationship began when, during the course of our investigations, the FBI recognized threat trends, tactics, and techniques involving Automated Clearing House (ACH) transactions and invited FS-ISAC representatives to receive a full FBI briefing. When the FBI asked the FS-ISAC whether this threat information would allow businesses and consumers to better protect themselves, reduce their vulnerabilities, and mitigate the consequences of these types of fraud, industry representatives advised that the information was pertinent and that a written product would be useful. In an entirely new collaboration model, we created a joint product in which the FBI wrote the first two sections involving the nature of the threat and how to recognize it and the FS-ISAC (working with the National ACH Association) wrote the second two sections regarding industry impact and security recommendations for preventing further fraud. The President of the FS-ISAC has highlighted this product as a successful example of government sector - private sector information sharing.

a. In what areas do you think improved cooperation would be helpful?

Response:

The FBI's ability to prevent and disrupt the cyber threats depends upon our ability to obtain threat information from the private sector, particularly from service providers. This is because service providers are often able to identify and characterize indications of threat activity (e.g., intrusions and other anomalous behavior) before the FBI becomes aware of the activity. As a result, it is vital that we maintain effective information sharing partnerships with private sector entities.

Although important, information sharing between the public and private sectors can be challenging because both see impediments to sharing with the other. For example, private sector victims of cyber events are sometimes hesitant to share proprietary information with law enforcement because they believe the information will be subject to public release pursuant to the Freedom of Information Act (FOIA) and thus will be available to their competitors. This perception persists notwithstanding our assurances that FOIA allows the government to withhold from disclosure six categories of information that was compiled for law enforcement purposes and information provided to the government that is confidential and commercial in nature. In addition to fearing the release of their proprietary information, private sector organizations may be

These responses are current as of 6/14/11

reluctant to share information regarding cyber intrusions because they believe their customers will fear for the security of their personal information if they learn that the organization has been victimized by a cyber intrusion.

There are also legal obstacles to the government's ability to share threat information with the private sector. For example, when the government obtains threat information through the grand jury process, the restrictions imposed by Rule 6(e) of the Federal Rules of Criminal Procedure may inhibit the disclosure of that information to concerned third parties in the private sector. In addition, the Electronic Communications Privacy Act (ECPA) prohibits wire, Electronic Communication Service (ECS), and Remote Computing Service (RCS) providers from voluntarily disclosing to the government records and other information pertaining to subscribers or customers of such services, including the contents of such communications, except in narrow circumstances. Specifically, disclosure can be made if the contents of the communication "appear to pertain to the commission of a crime" (18 U.S.C. § 2702(b)(7)(A)(ii)), the disclosure is "necessarily incident to . . . the protection of the rights or property of the provider" (18 U.S.C. §§ 2511(2)(a)(I), 2702(b)(5), and 2702(c)(3)), or the provider, in good faith, believes that an emergency involving danger of death or serious injury to any person requires disclosure without delay of information related to the emergency (18 U.S.C. § 2702(c)(4)).

b. What can Congress do to encourage this cooperation?

Response:

Legal clarity regarding the authority to share and to withhold information would create greater certainty and may improve willingness to share information in appropriate cases. For example, although the FBI believes most computer network exploitation (CNE) events will fall within one or more of the circumstances in which ECPA permits voluntary production, ultimately the decision to share this information must be made by the providers, who will be exposed to legal risk if they interpret the exceptions too broadly. In other words, the statute must afford the providers sufficient assurance that they will not incur liability if they share this information with the government. To the extent there is uncertainty whether the ECPA's exceptions apply to a suspected CNE, the statute creates a potential obstacle to the prompt sharing of threat information by ECS and RCS providers. Providers would presumably be more willing to voluntarily give the FBI access to ECPA-protected information where CNE is suspected if there were a clearer carve-out to cover that circumstance.

These responses are current as of 6/14/11

Questions Posed by Senator Hatch

Comprehensive Cyber Doctrine

4. Mr. Snow, I am concerned we do not have a comprehensive doctrine for Cybersecurity. During the Cold War our nation developed doctrines to deter the spread of communism and defined how the United States would react if attacked. Today, our policies are not nearly as clear. In the Cold War, the enemy also understood the theory of mutually assured destruction and strike back capability. However, in the cyber world, an enemy could hinder or eliminate our ability for retaliation in the first wave of a cyber attack. Fundamental questions have yet to be answered.

a. According to the FBI, what constitutes an attack against the United States?

Response:

While the FBI is a key partner in the comprehensive multi-agency response to cyber-based threats to our national security, investigating cyber-based terrorism, hostile foreign intelligence operations conducted over the Internet, computer intrusions targeting the national information infrastructure, and other cyber crime, we do not assess whether these intrusions constitute "attacks against the United States."

b. Since the FBI is both a law enforcement agency and a member of the U.S. Intelligence Community, how does the FBI weigh in on these issues?

Response:

In addition to investigating cyber crimes in furtherance of the FBI's law enforcement mission, the FBI's Cyber Division includes sections that focus specifically on matters related to our role in the U.S. Intelligence Community (USIC). For example, the Cyber Intelligence Section provides actionable intelligence in support of the Cyber Division's intelligence functions, while the Cyber National Security Section provides program management related to counterterrorism and counterintelligence computer intrusions. The FBI works through the Department of Justice and the Office of the Director of National

These responses are current as of 6/14/11

Intelligence (ODNI) to raise concerns and address policy matters related to both our law enforcement and intelligence roles.

c. How is intelligence information pushed up the line to policy makers and decision makers regarding attribution and identifying those responsible for the attack?

Response:

FBI intelligence is disseminated formally through standard USIC products (including Intelligence Information Reports, Intelligence Bulletins, and Intelligence Assessments) and is routinely incorporated into multi-agency products (including ODNI/National Intelligence Council products). In addition, the FBI works with the National Cyber Investigative Joint Task Force (NCIJTF) to develop tactical operational plans targeting those responsible for attacks, providing those plans to senior policy makers for review and approval. The FBI also routinely provides briefings to policy and decision makers within the Executive Branch, Congress, and the private sector.

National Cyber Investigative Joint Task Force

5. Hackers can simultaneously attack our critical infrastructure. These hacks impact banking systems, electrical grids, transportation systems and military networks. However, based on our organizational structure, the responsibility for defending these systems falls to a variety of different agencies. This could give the hacker an advantage unless information is shared. I am aware that the FBI leads the National Cyber Investigative Joint Task Force. This national center has personnel from a variety of agencies and entities assigned there, including the Secret Service. What is the dynamic inside the task force? Are agencies cooperating with one another?

Response:

The NCIJTF is a collaborative organization in which all participants are aware that cooperation is the key to success and are dedicated to ensuring that success. This task force enables the U.S. Government to execute a coordinated response to cyber threats by using domestic law enforcement and foreign intelligence authorities together in concert, coordinating and integrating the counterterrorism, counterintelligence, intelligence, and law enforcement activities of task force members. Although most of those who make up the NCIJTF are full-time task force members, some agencies are unable to dedicate a full-time cadre and instead

These responses are current as of 6/14/11

have their members attend only those meetings focused on threat topics of particular interest to that agency.

Because the task force's organization is designed to foster collaboration, its structure encourages the discovery of related intelligence and investigative targets, strengthened situational awareness of threat actors and motives, and faster and more reliable execution of intelligence and investigative objectives (such as determining threat attribution). The NCIJTF also facilitates the deconfliction of agencies' activities and the reconciliation of competing equities at a tactical level, often leading to more cooperative and mutually beneficial outcomes.

Challenges are inherent in the combination of agencies with different missions, authorities, focuses, and resources. Nonetheless, the close working environment and collaborative approach have been extremely successful, with significant work among key national cyber investigative and intelligence contributors leading to better awareness of the needs and goals of counterparts at other agencies and facilitating collaboration in circumstances where it might not otherwise have occurred. Many member agencies now find the NCIJTF an indispensable enabler of their own investigative or intelligence missions.

The NCIJTF's accomplishments have been acknowledged by the USIC. In August 2009, in recognition of the exceptional service of the NCIJTF's alliance of peers, operators, and analysts, who worked together on threats of concern from April 2007 to April 2009, the ODNI presented to the NCIJTF a National Intelligence Meritorious Award. The award acknowledged that the NCIJTF "was the driving force behind the transformation of cyber threats from a fragmented and reactive individual agency response, to a unified and highly successful proactive national effort that established itself as a national center of excellence."

These responses are current as of 6/14/11