THE FEDERAL BUREAU OF INVESTIGATION'S ABILITY TO ADDRESS THE NATIONAL SECURITY CYBER INTRUSION THREAT

U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 11-22
April 2011

REDACTED - FOR PUBLIC RELEASE

THE FEDERAL BUREAU OF INVESTIGATION'S ABILITY TO ADDRESS THE NATIONAL SECURITY CYBER INTRUSION THREAT

EXECUTIVE SUMMARY[1]

Computer systems integral to the infrastructure, economy, and defense of the United States are under constant attack by a growing array of adversaries. [redacted] For 2008, the Department of Homeland Security publicly reported 5,499 known intrusions of U.S. government computer systems alone, a 40 percent increase from 2007.

Because of its statutory authority, expertise, and responsibilities for counterterrorism, counterintelligence, and criminal law enforcement duties, the FBI plays a critical role in combating cyber threats.

Background

National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) (Presidential Directive NSPD-54/HSPD-23) assigned the Secretary of Homeland Security and the Attorney General the responsibility for ensuring adequate support for the agents, analysts, and technical infrastructure to neutralize, mitigate, and disrupt illegal computer activity aimed at domestic targets. In 2008, the

[1] The Office of the Director of National Intelligence (ODNI) coordinated with Intelligence Community agencies, including the FBI, and identified within the full version of this report classified and other information that if released publicly could compromise national security interests and the FBI's operations. To create this public version of the report, the OIG redacted (blacked out) these portions of the full report.

The effort to identify classified information in this report has been a significant factor delaying the release of this report. Originally, the FBI reviewed a draft of this report for classified material and provided the OIG the results of this review on November 4, 2010, at which time the FBI stated that the report also required a classification review for information pertaining to subject matter that is outside the FBI's classification authority. The ODNI provided the results of this review on March 17, 2011. We reviewed the ODNI's classification review and believed the classification markings and redactions were over-inclusive. We coordinated with the FBI and ODNI, and on April 18, 2011, we reached a consensus on the final determination on the classification of information in the full report.

President established the Comprehensive National Cybersecurity Initiative (CNCI) to implement the responsibilities outlined in the Presidential Directive.

The CNCI is intended to combine the missions of various federal agencies to defend against cyber intrusions [redacted] The FBI conducts investigations into computer intrusions as defined in 18 USC § 1030, which states that a computer intrusion as actual or attempted unauthorized access of a protected computer, which includes any computer connected to the internet or any computer connected to a network that is connected to internet. According to Cyber Division guidance on conducting and classifying cyber investigations, a national security intrusion is one conducted by foreign powers for intelligence or terrorist purposes.[2]

Through the CNCI the FBI was assigned with ensuring adequate support to neutralize, mitigate, and disrupt illegal computer activity aimed at domestic targets.[3]

The FBI's Cyber Division has primary responsibility for the FBI's efforts to counter national security-related cyber intrusions. Within the Cyber Division, the Cyber National Security Section oversees the FBI's national security cyber intrusion efforts. The FBI combats cyber intrusion threats primarily through two operational components: the National Cyber Investigative Joint Task Force (NCIJTF), an FBI-led multi-agency task force recognized by the CNCI, and FBI cyber investigative squads located in each FBI field office.

The NCIJTF is charged with ensuring that the U.S. government coordinates its efforts to address national security cyber intrusions, including intelligence operations and investigations. The FBI is the lead agency and

[2] According to the FBI, cyber crime also threatens U.S. national security interests. As a result, the FBI's Computer Intrusion Program and the National Cyber Investigative Joint Task Force both have criminal-based, law enforcement components.

[3] To accomplish its goals, the CNCI includes 12 interdependent initiatives. A complete description of the CNCI initiatives is contained in Appendix III.

operational manager of the NCIJTF, which includes 18 intelligence community and law enforcement agencies.[4]

Each of the 56 FBI field offices throughout the United States has at least one cyber squad consisting of special agents, intelligence analysts, and in some cases linguists and computer scientists. The largest field offices have multiple cyber squads, with each squad responsible for investigating different types of cyber cases – such as national security intrusions, criminal intrusions, online child pornography, intellectual property rights, and internet fraud. In the small to medium size field offices, a single cyber squad may be responsible for investigating all types of cyber cases.

Audit Approach

The objectives of this audit were to: (1) evaluate FBI efforts in developing and operating the National Cyber Investigative Joint Task Force (NCIJTF) to address the national security cyber threat; and (2) assess FBI field offices' capabilities to investigate national security cyber cases. These objectives focused mainly on the FBI's highest cyber priority, counterterrorism and counterintelligence intrusions.[5]

We conducted field work at FBI headquarters in Washington, D.C., the NCIJTF, and at 10 of the FBI's 56 field offices. We interviewed officials from the FBI Cyber Division and representatives from the FBI's partner agencies at the NCIJTF. In the 10 field offices we visited, we interviewed FBI special agents responsible for managing cyber squads and investigating national security intrusion cases, as well as 36 agents who conduct these investigations. We also examined the education, work experience, and training for each special agent interviewed to evaluate the agents' ability to adequately investigate national security intrusion cases. We also reviewed the NCIJTF's Quarterly Progress Reports to determine the FBI's progress in meeting the CNCI implementation goals. Appendix I contains a more detailed description of our audit objectives, scope, and methodology.

[4] Appendix IV contains a list of participating NCIJTF agencies. Although 18 agencies participate in the NCIJTF, as of June 2010 only 12 of the 18 had signed a memorandum of understanding (MOU) establishing each agency's membership and addressing information sharing and other legal concerns.

[5] The Cyber Division priorities in rank order are: (1) cyber intrusions, (2) child sexual exploitation, (3) intellectual property rights, and (4) internet fraud.

Results in Brief

We found that the FBI has completed the interim goals for the NCIJTF as developed under the CNCI and has identified techniques and tactics being used to attack U.S. computer networks. The FBI developed an operational plan for the NCIJTF, established threat focus cells to address specific cyber threats, incorporated many Intelligence Community and law enforcement partners into the day-to-day operations of the NCIJTF, and has had some operational successes in mitigating cyber threats against the United States.[6]

Despite these accomplishments, the NCIJTF needs to continue to improve its capabilities to combat cyber attacks.

For example, the NCIJTF was not always sharing information about cyber threats among the partner agencies participating in the NCIJTF. Partner agencies are co-located at the NCIJTF and are expected to work together daily on mitigating and neutralizing the cyber threat against the United States. Much of the information sharing at the NCIJTF occurred during threat focus cell meetings, where member agencies share new information that their agencies have gathered about a specific type of cyber threat. However, some agencies were often asked to leave threat focus cell meetings.

Moreover, because the NCIJTF is an interagency task force, we believe it is vital that all of the partner agencies have common understandings about information sharing. The FBI recognized this need and uses a memorandum of understanding (MOU) that outlines the framework for information sharing among NCIJTF members. As of June 2010, the 4 presidentially-mandated partner agencies and 8 of the 14 additional partner agencies at the NCIJTF had signed the memorandum. In addition, we found that the MOU signed by the partner agencies contains a much more restrictive information sharing policy than described in the NCIJTF Operational Plan. The FBI stated that the MOU is consistent with the NCIJTF Operational Plan, but the MOU is more detailed and recognizes statutory and policy limitations to information sharing that member agencies must uphold.

We also found that, despite the CNCI requirement that the National Security Agency (NSA) be fully integrated into the NCIJTF,

[6] Threat focus cells are investigative management teams that concentrate on specific intrusion threats to eventually identify persons responsible for the intrusions.

[redacted]. For example, [redacted] Additionally, during our review [redacted], and the FBI believed that participation from another [redacted]. In response to a draft of our report, the FBI stated that the NSA has since added a representative from a second operational component.

In addition, our audit found that of the 36 agents we interviewed at the 10 field offices we visited, 64 percent of the agents assigned national security-related cyber investigations reported having the expertise needed to investigate these types of cases. The remaining 36 percent of these field agents reported that they lacked the networking and counterintelligence expertise to investigate national security intrusion cases. Moreover, five of the field agents we interviewed told us that they did not think they were able or qualified to investigate national security intrusions effectively. In addition, the FBI's rotation policy, which rotates agents among different FBI offices to promote a variety of work experience, hindered the ability [redacted] to investigate national security intrusions.[7] We also found that the forensic and analytical capability in the field offices was inadequate to support national security intrusion investigations. Some field agents believed this affected the FBI's ability to determine those responsible for intrusions.

The remaining sections of this Executive Summary summarize our audit findings.

National Cyber Investigative Joint Task Force

On January 8, 2008, the President signed Presidential Directive NSPD-54/HSPD-23, which named the FBI as its lead agency of the NCIJTF and directed the NCIJTF to serve as a multi-agency, national focal point for coordinating, integrating, and sharing pertinent information related to cyber

[7] A 2007 U.S. Government Accountability Office (GAO) report also found that the FBI's rotation policy reduced the number of qualified cyber agents assigned to conduct cyber investigations.

threat investigations. The NCIJTF is the FBI's centralized effort related to its national security-related cyber intrusion efforts. According to an Office of the Director of National Intelligence official responsible for overseeing the implementation of the CNCI, the NCIJTF is a prototype of what was intended when the CNCI was created – that is, to ensure multiple federal agencies with cyber authorities work together and share intelligence to mitigate and neutralize the cyber threat against the United States.

In March 2008 the Office of the Director of National Intelligence issued a report on the CNCI (CNCI report) that outlined the goals, plans, and performance measures for the first 3 years of the CNCI implementation, with interim milestones for developing NCIJTF at designated intervals throughout the 3-year period.[8] During our audit, we found that the FBI had met many of the interim milestones.[9] For example, in April 2008 the FBI completed the NCIJTF Operational Plan, which established the organization's mission, identified the task forces' participating agencies, outlined the NCIJTF's structure, and proposed an information sharing methodology to be used by task force partners.[10] In addition, the three agencies directed by the Presidential Directive to participate with the FBI in the NCIJTF – [redacted] NSA, and U.S. Secret Service – are all participating in the NCIJTF.

According to the CNCI report, performance measures for the NCIJTF include the number of: [redacted]

In addition to completing many of the CNCI report's requirements and performance goals, the NCIJTF conducted successful cyber intrusion

[8] Office of the Director of National Intelligence, *The Comprehensive National Cybersecurity Initiative: Goals, Plans, and Performance Measures*, (March 2008). This report was submitted to the Office of Management and Budget.

[9] In January 2011, following its November 2010 response to our report, the FBI provided the OIG an October 2010 report that it submitted to the Office of the Director of National Intelligence, which described the FBI's most recent actions to implement the NCIJTF and fully achieve the March 2008 development milestones.

[10] The background section of this report outlines in detail the NCIJTF's mission and structure.

cases during its first 18 months.[11] [redacted]

Information Sharing at the NCIJTF

While the FBI has made progress in developing the NCIJTF, information sharing at the NCIJTF is hindered by legal restrictions and policy limitations. The NCIJTF was intended to promote interagency access to and sharing of information about cyber threats. However, we found that task force members first attempted to determine the relevancy and importance of its information to another agency's operations before sharing that information with another agency. For example, a Naval Criminal Investigative Service (NCIS) representative to the NCIJTF told us that the FBI did not share information relevant to an NCIS investigation of an [redacted]. The FBI stated that it did provide this information to the NCIS about 5 months following our discussion with the NCIS representative. Additionally, we were told that some agencies are often asked to leave threat focus cell meetings when certain information is being shared. This approach to information sharing prevents some NCIJTF partners from being fully-integrated partners.

The FBI has no legal authority to require its NCIJTF partners to share information. However, the FBI recognized the need for agencies participating in the NCIJTF to agree on the principles for information sharing at the NCIJTF and developed an information sharing framework for the NCIJTF. The FBI asked each participating agency to sign an MOU stating that it will abide by the NCIJTF's information sharing framework. However, as of June 2010, the 4 presidentially-mandated partner agencies – the FBI, [redacted] NSA, and U.S. Secret Service – and 8 of the additional 14 partner agencies had signed the NCIJTF MOU. The other signers are the Air Force Office of Special Investigation and Defense Security Service, Naval Criminal Investigative Service, Department of Energy, Department of State, Joint Task Force – Global Network Operations, National Geospatial Intelligence Agency, and Department of Homeland Security – US CERT.[12] The Department of Justice (Department),

[11] The details of the NCIJTF's cases are classified at a higher level than this report and, therefore, are not included in this report.

[12] The following 6 agencies that participate at the NCIJTF have not signed an MOU: Department of Justice, U.S. Army 902nd Military Intelligence Group, U.S. Army Intelligence and Security Command, Defense Intelligence Agency, U.S. Army Criminal Investigative Division, and Defense Criminal Investigative Service.

although a participating agency at the NCIJTF, has not signed an MOU. According to the Department's liaison to the NCIJTF and the NCIJTF Deputy Director, the Department is not required to sign an MOU because the Department does not have personnel assigned to work at the NCIJTF. Instead, the Department's role at the NCIJTF is that of legal consultant, and it does not participate in the day-to-day operations of the NCIJTF.

In addition, in the 12 signed MOUs, we found that the information sharing language of the MOUs was more restrictive than the information sharing framework described in the NCIJTF Operational Plan. The Operational Plan states that information shared outside the NCIJTF must have the approval of the agency that collected the information originally. According to Cyber Division Assistant Director, the Operational Plan was designed to maximize information sharing within the NCIJTF, but it also gives member agencies control over when information they collected is disseminated outside the NCIJTF. However, the MOUs also contain restrictive policy for sharing information within the task force, stating that each agency decides the information it will share and not share.

In its response to the working draft report, the FBI stated that the MOU is consistent with the NCIJTF Operational Plan, and it recognizes statutory and policy limitations to information sharing that member agencies must uphold, which is consistent with the Attorney General Guidelines for the NCIJTF. In our opinion, the FBI should ensure that all member agencies are aware of the statutory and policy limitations to information sharing at the NCIJTF to avoid misunderstandings surrounding the sharing of information.

Integrating the Intelligence Community

Until July 2009, of the four agencies directed in the Presidential Directive to provide representatives to the NCIJTF, the FBI, U.S. Secret Service, [redacted] had assigned permanent cyber personnel with responsibilities for the day-to-day operations of the NCIJTF. [redacted]

After the NSA assigned a permanent representative to the NCIJTF, we found that [redacted]

[redacted]. The NSA representative told us that she [redacted] In response to a draft of our report, the FBI said that it is not the NCIJTF's practice to invite members to threat focus cell meetings. Instead, threat focus cell meetings are posted on a display in the entryway and announced at weekly or biweekly NCIJTF-wide meetings. [redacted]

Additionally, the [redacted] The NSA stated that it originally decided to [redacted] at the NCIJTF because it wanted the NCIJTF to work through that single component for all NSA support. In response to a draft of this report, the FBI stated that the NSA has assigned to the NCIJTF a representative from this component. In November 2010, [redacted]

Field Office Capabilities

While the NCIJTF is the headquarters component of the FBI's national security cyber intrusion efforts, the FBI's 56 field offices primarily conduct the investigation of national security cyber intrusions. As a result, the field agents assigned to investigate national security intrusions need to understand the current techniques and tactics used in cyber intrusions. In the FBI field offices we visited we found that 64 percent of the FBI cyber agents we interviewed who were assigned to work national security cyber intrusion cases reported having sufficient education, prior work experience, or technical capabilities to investigate this type of high-priority intrusion. However, our audit found agents assigned to investigate national security cyber intrusion cases who did not believe they were qualified to investigate these cases effectively.

In January 2007, the FBI issued the Cyber Development Plan, a roadmap for agents in the Cyber Career Path to become experts in cyber investigations that includes 12 core courses and an elective curriculum. The Cyber Development Plan is divided into four stages, each of which requires agents to complete specific training courses and have experience with FBI procedures and investigative techniques. The Cyber Division defines a quality cyber agent as one who has completed the training courses in stages 3 or 4 and who can describe how to competently address Cyber Division's three types of priority cases. As of June 2010, [redacted]

[redacted] cyber agents had completed or tested out of all 12 core courses of the development plan. In response to a draft of our report, the FBI stated that it expects agents to complete the 12 core courses and the on-the-job training required by the development plan in 5 to 7 years.

We also found that the staged format of the development plan can impede an agent's ability to acquire the training necessary to investigate national security intrusion cases effectively. According to FBI officials, agents assigned to national security cyber intrusion matters need to have more advanced technical capabilities than agents investigating other cyber matters, such as online child pornography and intellectual property rights. However, we found that the courses most beneficial to agents investigating national security investigations are not offered to the agents until the latter stages of the Cyber Development Plan, when agents have been in the cyber career path for 3 years. In its response to a draft of this report, the FBI stated that it does allow agents to bypass prerequisites normally necessary to ensure background knowledge when more advanced classes are pertinent to their current case assignment.

In addition to coursework, each stage of the Cyber Development Plan includes on-the-job training elements. We found that the design of the development plan had a disproportionately large impact on the FBI's smaller field offices. Because smaller offices are staffed mostly with newly-hired agents, these offices may not be able to provide new agents with a mentor qualified in the investigation of national security intrusions. Therefore, these new agents may not have the opportunity to complete the on-the-job training elements of the Cyber Development Plan.

To assess the qualifications of current cyber agents to investigate national security cyber intrusion matters, we tested whether the 36 cyber agents we interviewed had the technical skill set that Cyber Division officials said were necessary to investigate national security intrusions.[13] We found that 23 (64 percent) of these agents we interviewed had these technical skills. We also examined each of these 36 agents' prior work experience and formal education and found that 18 of these 36 had prior work experience in computer networking, which Cyber Division officials said was especially valuable to performing national security cyber investigations effectively.[14] In addition, although the NCIJTF is the centerpiece of the FBI's national

[13] The 36 special agents we interviewed were selected because they had national security intrusion responsibilities within their field office cyber squad.

[14] The other degrees included accounting, engineering and mathematics, law, politics, criminal justice, sociology, and psychology.

security cyber intrusion operations, approximately 36 percent of the 36 FBI cyber agents we interviewed had not heard of the NCIJTF.

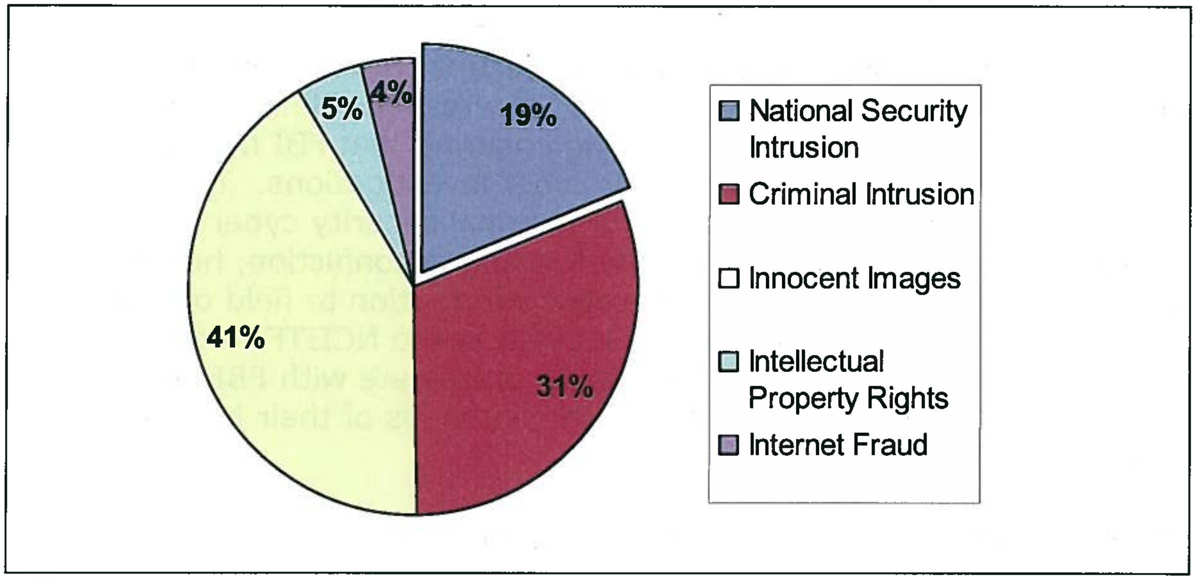
The Cyber Division's Cyber National Security Section program managers, who are located at the NCIJTF, are responsible for coordinating FBI investigations on a national level and ensuring that FBI field agents have sufficient information pertinent to their cyber investigations. These program managers are important to all stages of national security cyber intrusion investigations, in identifying trends, performing deconfliction, helping ensure coordination, and providing other valuable information to field offices. However, the five program managers located at the NCIJTF whom we interviewed said they could not sufficiently coordinate with FBI field offices because they did not have time due to the demands of their NCIJTF-related workload.

Field Office National Security Cyber Intrusion Efforts

Five of the 36 field agents we interviewed told us that they did not think they were able to investigate national security intrusions effectively and that they were not qualified to investigate national security intrusions. One agent who had recently been assigned his first counterterrorism intrusion case said that he did not know how to investigate a national security intrusion case. He was concerned about his ability to perform the investigation, especially because he viewed it as a significant case.

Overall, we determined that in FY 2009 the FBI used 19 percent of its cyber agents on national security intrusion investigations, 31 percent to address criminal-based intrusions, and 41 percent to investigate online child pornography matters.

UTILIZATION OF AGENTS ON CYBER INVESTIGATIONS FISCAL YEAR 2009[15]



Source: Federal Bureau of Investigation

For the 10 field offices we visited, the FBI allocated [redacted] special agents to investigate cyber cases in FY 2009. These 10 offices assigned [redacted] of the [redacted] agents (34 percent) to investigate national security intrusion cases. However, we found that as of September 2009 only [redacted] of the [redacted] agents (45 percent) were actively investigating national security intrusions.

Rotation Policy

The FBI's special agent rotation policy calls for a new agent [redacted] to rotate [redacted] after 3 years. When an agent transfers from a field office, the agent's cases are reassigned to other agents in that field office, often to agents in their first assignments out of the FBI Academy.

FBI officials said the FBI's rotation policy is based on traditional crime priorities, where the FBI's smaller field offices often conduct smaller scale and less complex investigations than those encountered at the FBI's larger field offices. However, national security intrusions do not conform to this traditional model because they are not concentrated in any particular area of the country and do not vary in complexity by locale. When a foreign

[15] According to Cyber Division guidance on conducting and classifying cyber investigations, a national security intrusion is one conducted for intelligence or terrorist purposes by foreign powers, including international terrorist groups. Criminal intrusions are those motivated for criminal conduct.

country uses computer networks to attack a cleared-defense contractor in Memphis, it uses the same technology and techniques to attack a cleared-defense contractor in New York. As a result, the FBI field offices in Memphis and New York, for instance, need agents equally well-qualified in investigating national security intrusions.

The GAO found in a June 2007 review that the FBI's rotation policy had a negative impact on the capabilities of field office cyber squads.[16] The GAO reported that when cyber crime agents transferred from one office to another as part of the FBI's rotation policy these agents were not necessarily reassigned to cyber crime investigations in their new field offices, leaving their cyber background underutilized. In addition, the GAO found that the agents who replaced experienced cyber crime investigators often had little or no cyber crime experience or background. We found during our review that this condition still existed in FBI field offices. The FBI stated that in order to augment cyber squads [redacted], in FY 2010, it canvassed its field divisions and [redacted] experienced cyber agents throughout the field. An additional canvass to determine needs for experienced cyber agents was planned for November 2010.

Because national security intrusion cases are highly technical and require a specific skill set, new cyber agents are often not equipped to assume responsibility of a national security intrusion investigation. During our field office visits, we interviewed cyber career path agents in their first assignments after graduating from the FBI Academy who had assumed national security intrusion cases after their predecessors rotated to other field offices. These new agents told us they did not believe they had the technical expertise and investigative experience to adequately investigate the ongoing national security intrusions they had assumed. In 4 of the 10 offices we visited, agents told us they had been assigned cyber cases that exceeded their technical capabilities.

Most FBI special agents we interviewed said that classroom instruction on cyber intrusions is valuable, but they emphasized that practical experience was necessary to best develop an agent to investigate national security intrusions effectively. In addition, these agents said the rotation policy compounded their challenge because experienced cyber agents were often rotated to another office, leaving new agents without experienced agents to train or mentor them on the unique aspects of investigating national security intrusions.

[16] GAO, CYBERCRIME: Public and Private Entities Face Challenges in Addressing Cyber Threats, GAO-07-705 (June 2007).

After we concluded our audit fieldwork and noted our concern to the FBI about the difficulty [redacted] field offices have in staffing their cyber squads adequately, the FBI reviewed the number of allocated cyber agents at the FBI's 56 field offices. The FBI concluded that [redacted] field offices received more cyber agents than they needed, while [redacted] offices did not have sufficient cyber personnel. This internal FBI review also attributed the staffing difficulties [redacted] to the FBI's rotation policy. As a result of this review, the Cyber Division is now allowing qualified cyber agents to transfer [redacted] offices, removing agents who do not have sufficient cyber skills from the career path, and selecting only those agents with significant cyber education or skills for the cyber career path.

Analytical Support

The FBI's Directorate of Intelligence manages the FBI's intelligence program and intelligence analysts. It is important for the FBI's Cyber Division and Directorate of Intelligence to work together to ensure that field office cyber squads have the tactical analytical support necessary to investigate national security cyber intrusions successfully.

In March 2008, the FBI launched its new Field Intelligence Model, which called for embedding intelligence analysts within FBI operational squads to ensure the coordination of investigative and intelligence operations.[17] This included a plan to embed intelligence analysts within the field office cyber squads.

However, our review determined that intelligence analysts were not always embedded with the field office's cyber squads and that when they were embedded, FBI field agents did not receive the tactical analytical support for national security intrusion investigations from intelligence as called for by the Field Intelligence Model. Moreover, contrary to the Field Intelligence Model, intelligence analysts we interviewed stated that their role is to provide a strategic or overall threat analysis and not to provide tactical or case-specific support. Some of the cyber agents we interviewed said that insufficient tactical analytical support hampered their ability to connect the dots in an investigation, further limiting their ability to determine who was responsible for the intrusion.

[17] FBI Strategic Execution Team, *The New Field Intelligence Model*, Version 1.0, March 2008 – March 2009.

In this report, we make 10 recommendations to assist the FBI in preparing the NCIJTF and its field agents to more adequately investigate national security intrusion cases and advance the nation in the fight against the national security cyber threat.

THE FEDERAL BUREAU OF INVESTIGATION'S ABILITY TO ADDRESS THE NATIONAL SECURITY CYBER INTRUSION THREAT

TABLE OF CONTENTS

INTRODUCTION

Computer systems integral to the infrastructure, economy, and defense of the United States are under constant attack. For example, the Director of National Intelligence stated in February 2010 that sensitive information is stolen daily from both government and private sector networks.[18] Certain nation states, terrorist groups, organized criminal groups, unethical foreign corporations and businesses, disaffected individuals, and hackers present continuous cyber threats to the United States. Some of them have the capability to compromise, steal, change, and destroy information that could cause critical disruptions to systems belonging to the federal government, government contractors, and private companies, including financial institutions and utilities. [redacted] For 2008, the Department of Homeland Security publicly reported 5,499 known intrusions of U.S. government computer systems alone, a 40 percent increase from 2007.

In 2008, in response to the growing cyber threat, the President established the Comprehensive National Cybersecurity Initiative (CNCI). The CNCI is a multi-agency, phased approach to addressing current cybersecurity threats, anticipating future threats and technologies, and developing innovative public-private partnerships that can help prevent, deter, and protect against cyber threats. The CNCI is intended to coordinate and integrate the work of federal government agencies involved in law enforcement, intelligence, military, diplomacy, and homeland security to defend against cyber intrusions [redacted].[19]

The FBI plays a critical role in the CNCI strategy to neutralize, mitigate, and disrupt illegal domestic computer activity. The CNCI states that the FBI is in a unique position to counter cyber threats as it is the only agency with the statutory authority, expertise, and ability to combine

[18] Blair, Dennis C., Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community for the House Permanent Select Committee on Intelligence (February 3, 2010).

[19] To accomplish its goals, the CNCI includes 12 interdependent initiatives. A complete description of the CNCI initiatives is contained in Appendix III.

counterterrorism, counterintelligence, and criminal resources in support of the CNCI.

FBI Cyber Division

In 2002, the FBI created its Cyber Division to focus resources and efforts on cyber-related operations.[20] The Cyber Division's Cyber National Security Section oversees the FBI's national security cyber intrusion effort – which is the FBI's highest cyber priority. The Cyber Division defines a computer intrusion as actual or attempted unauthorized access of a protected computer, which includes any computer connected to the internet or any computer connected to a network that is connected to the internet. A national security intrusion is one conducted by foreign powers or international terrorist groups for intelligence or terrorist purposes.[21] The Cyber Division priorities in rank order are: (1) cyber intrusions, (2) child sexual exploitation, (3) intellectual property rights, and (4) internet fraud.

The FBI primarily combats the cyber intrusion threat through two operational components: the National Cyber Investigative Joint Task Force (NCIJTF) and cyber investigative squads located in each FBI field office.[22]

According to the Cyber Division's Program Investigative Guide, the Cyber National Security Section directs FBI field offices in initiating counterterrorism and counterintelligence cyber investigations on the basis of information received from partner agencies; supports the development of cyber operations in the field; and coordinates field offices' national security-related cyber intrusion operations with other FBI divisions, domestic and international law enforcement agencies, and intelligence community partners.

[20] Appendix II depicts the FBI Cyber Division's organization structure.

[21] According to the FBI, cyber crime also threatens U.S. national security interests. As a result, the FBI's FBI Computer Intrusion Program and the National Cyber Investigative Joint Task Force each have criminal-based, law enforcement components.

[22] The NCIJTF is one of six cybersecurity centers named in the CNCI. The other five cybersecurity centers are: (1) National Security Agency Threat Operations Center, (2) Department of Defense's Joint Task Force – Global Network Operations, (3) Department of Homeland Security's U.S. Computer Emergency Readiness Team, (4) Department of Defense's Defense Cyber Crimes Center, and (5) Director of National Intelligence's Intelligence Community Incident Response Center.

National Cyber Investigative Joint Task Force

Through the NCIJTF, the FBI's Cyber National Security Section coordinates with 18 other national security and intelligence community partner agencies to combat cyber intrusions.[23] The FBI serves as the lead agency and operational manager of the NCIJTF and the FBI Section Chief of the Cyber National Security Section also serves as the NCIJTF Director.[24]

The mission of the NCIJTF is to ensure that the U.S. government is coordinating all its efforts to address national security cyber intrusions, including intelligence operations and investigations. The NCIJTF's functions are structured in three groups: the Information Operations Group, the Analysis Group, and the Law Enforcement Group. The Information Operations Group is responsible for ongoing operational efforts and developing and refining investigative leads distributed to field elements. The Analysis Group focuses on developing, maintaining, and disseminating actionable strategic intelligence products.

Close coordination and collaboration within the NCIJTF is vital to its success. For this effort, partner agencies' representatives are co-located at the NCIJTF and work together on a daily basis. Representatives to the NCIJTF still have program management and coordination authority within their home agencies, which enables them to redirect their agency's cyber threat investigation activities based on the information gleaned from NCIJTF operations. The NCIJTF is also intended to enhance the FBI's ability to achieve its intelligence gathering and investigative missions by providing actionable intelligence to, and developing joint operations with, its federal partners.

One goal of the NCIJTF was to acquire facilities that could accommodate representatives from all participating agencies as well as a 24/7 joint-operations center. The capacity of the NCIJTF's current facility has already been exceeded and partner agencies have requested accommodations for additional personnel to participate in the NCIJTF on a full-time basis. However, the FBI is unable to provide space for these potential participants. As of June 2010, the General Services Administration was in the process of negotiating final infrastructure requirements to

[23] While 18 agencies are participating at the NCIJTF, as of June 2010, the 4 presidentially-mandated agencies and 8 of the 14 additional partner agencies had signed a memorandum of understanding establishing each agency's membership and addressing information sharing and other legal concerns.

[24] Appendix IV contains a list of agencies participating in the NCIJTF.

relocate the NCIJTF in a new facility. The FBI expects the NCIJTF to occupy the new facility in March 2012.

Field Office Cyber Squads

Each of the FBI's 56 FBI field offices throughout the United States has at least one cyber squad consisting of special agents, intelligence analysts, and, in some cases, computer scientists and linguists. In the largest field offices, there are multiple cyber squads with each squad responsible for investigating different types of cyber cases – such as national security intrusions, criminal intrusions, online child pornography, intellectual property rights, and internet fraud. In the small to medium size field offices, a single cyber squad may be responsible for investigating all types of cyber cases.

National security intrusion cases can be referred to FBI cyber squads in several ways, including through victim complaints, private internet security companies, financial institutions, academia, other government agencies, and other FBI divisions such as the Counterterrorism Division or the Criminal Investigative Division.

After becoming aware of an intrusion, the FBI generally seeks to obtain consent from the victim to monitor the compromised network and collect and analyze the network's traffic to identify who is responsible for the intrusion and what information within the system is being targeted. FBI special agents often must analyze a terabyte or more of network traffic during the investigation of a national security intrusion case.[25] In addition, agents are expected to recruit and manage confidential informants or persons who have knowledge of such intrusions.

OIG Audit Approach

The objectives of this audit were to: (1) evaluate FBI efforts in developing and operating the NCIJTF to address the national security cyber threat; and (2) evaluate the FBI's field offices' capabilities to investigate national security cyber cases.

We conducted field work at FBI headquarters in Washington, D.C., the NCIJTF, and at 10 of the FBI's 56 field offices. The 10 FBI field offices we visited included small, medium, and large offices with varying numbers of

[25] A terabyte is about one trillion bytes or about 1,000 gigabytes.

national security intrusion cases.[26] We interviewed officials from the FBI Cyber Division and representatives from the FBI's partner agencies at the NCIJTF. In the 10 field offices we visited, we interviewed FBI special agents responsible for managing cyber squads and 36 agents performing the investigations of national security intrusion cases. We also examined the education, work experience, and training for each special agent interviewed to evaluate the agent's ability to investigate national security intrusion cases adequately. We also reviewed the NCIJTF's Quarterly Progress Reports to determine the FBI's progress in meeting the requirements of the CNCI. Appendix I contains a more detailed description of our audit objectives, scope, and methodology.

Prior Report

In June 2007, the U.S. Government Accountability Office (GAO) issued a report that addressed public and private entities' challenges in addressing cyber threats.[27] The report stated that federal law enforcement, including the FBI, faced a challenge in recruiting individuals with specialized skills and tools to investigate cyber crime. In addition, the GAO found that the available pool of experienced FBI cyber crime investigators was affected by its rotation policy. When cyber crime investigators rotate from one field office to another under the FBI's rotation policy, they are not necessarily reassigned to cyber crime investigations in the new field office, and their cyber background is underutilized. In addition, the agents who rotate in to replace experienced cyber crime investigators may have little or no cyber crime experience or background.

The GAO recommended that the Attorney General direct the FBI to assess the impact of the rotation approach on its abilities to investigate and prosecute cyber crime and to modify its approach, as appropriate. The FBI stated in its response that the rotational policies were approved after careful consideration of the viable alternatives provided by an analysis and study conducted by the Human Resources Division. In addition, the FBI stated that it had established five distinct career paths for both new and veteran special agents, including a specific designation for cyber matters. According to the FBI, the career path for cyber matters would ensure that the FBI recruits, trains, and deploys special agents with the critical cyber skill set

[26] Please see Appendix I for a detailed description of the methodology we used to select the 10 field offices. The 10 field offices we visited were [redacted].

[27] U.S. Government Accountability Office (GAO), CYBERCRIME: Public and Private Entities Face Challenges in Addressing Cyber Threats, GAO-07-705 (June 2007).

required to keep the FBI on the cutting edge of computer technology and development, and positioned to counter the constantly evolving cyber threat.

The GAO concluded that despite efforts to assess and expand analytical and technical capabilities, the rotational policies may adversely affect the FBI's use of staff with cyber expertise. The GAO recommended that the FBI continually reassess what impact the rotational policy had on the FBI's ability to address the cyber threat.

FINDINGS AND RECOMMENDATIONS

Finding I: National Cyber Investigative Joint Task Force

> The FBI has made progress developing the National Cyber Investigative Joint Task Force (NCIJTF). It developed an operational plan for the NCIJTF, established threat-focus cells to address specific cyber threats, and began to incorporate its intelligence community partners into day-to-day NCIJTF operations. However, we found that the FBI and other NCIJTF member agencies did not consistently share information on cyber intrusion cases, and in those cases where information was not shared NCIJTF partners were not told why they did not receive available information. We also determined that the FBI needs to enhance the coordination between its field offices and the NCIJTF regarding national security cyber intrusions. Further, NCIJTF agencies could be better integrated into the task force's operations. We also determined that several NCIJTF partner agencies had not signed a memorandum of understanding (MOU) establishing information sharing protocols among the NCIJTF partners.

In June 2005, the Cyber Investigative Joint Task Force was established as a partnership between the FBI and the Department of Defense Cyber Crime Center to address cyber intrusions that had national security implications and [redacted]. In July 2007, the FBI's Cyber and Counterintelligence Divisions assumed responsibility for the Cyber Investigative Joint Task Force, expanded its scope, and renamed it the National Cyber Investigative Joint Task Force (NCIJTF).

On January 8, 2008, the President signed National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Presidential Directive NSPD-54/HSPD-23). The Presidential Directive directed the NCIJTF to serve as a multi-agency, national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations. The Presidential Directive assigned the FBI responsibility for developing the NCIJTF. Additionally, the directive ordered the [redacted] National Security Agency (NSA), U.S. Secret Service (Secret Service), and other agencies, as appropriate, to participate in the NCIJTF.

In March 2009, the FBI reorganized its Cyber Division and created the Cyber National Security Section. The Cyber National Security Section manages the FBI's counterterrorism and counterintelligence computer intrusion operations for FBI field offices and for the NCIJTF.

To streamline the FBI's responsibilities and support its field offices' national security cyber activities, the FBI co-located the Cyber National Security Section with the NCIJTF and appointed the Section Chief of the Cyber National Security Section to also serve as the NCIJTF Director. Program managers within the Cyber National Security Section serve as the FBI's representatives to the NCIJTF, and also provide support to FBI field office cyber investigations, and manage daily NCIJTF activities. FBI field offices are the primary contributors of investigative intelligence to the NCIJTF.

The NCIJTF is critical to the success of FBI cyber operations as well as to overall U.S counterintelligence cyber operations. According to an Office of the Director of National Intelligence official responsible for overseeing the implementation of the CNCI, the NCIJTF is a prototype of what was intended when the CNCI was created – that is, to ensure multiple federal agencies with cyber authorities work together and share intelligence to mitigate and neutralize the cyber threat against the United States.

NCIJTF Development

In March 2008 the Office of the Director of National Intelligence (ODNI) issued a report to the Office of Management and Budget that outlined the goals, plans, and performance measures for the first 3 years of the CNCI implementation (CNCI report), with interim milestones for developing the NCIJTF at designated intervals throughout the 3-year period.[28] As shown in Exhibit 1-1, we found that through March 2010 the FBI had met many of the interim milestones. For example, in April 2008 the FBI completed the NCIJTF Operational Plan, which established the organization's mission, identified the task forces' participating agencies, outlined the NCIJTF's structure, and proposed an information sharing methodology to be used by task force partners. Additionally, as of July 2009, the FBI integrated into NCIJTF operations the [redacted] NSA, and U.S. Secret Service, as required by Presidential Directive NSPD-54/HSPD-23. At the time we issued a draft of this report to the FBI in October 2010, to our knowledge, the FBI was still in the process of accomplishing certain milestones for developing the NCIJTF. In January 2011, following its

[28] Office of the Director of National Intelligence, *The Comprehensive National Cybersecurity Initiative: Goals, Plans, and Performance Measures*, (March 2008).

November 2010 response to our report, the FBI provided the OIG with its CNCI 4th Quarter 2010 Quarterly Report, which described to the ODNI the FBI's most recent actions to implement the NCIJTF. The FBI reported to ODNI that it has completed all NCIJTF development milestones as outlined in March 2008.[29]

[29] In this report, we recommend that the FBI ensure the completion of the activities for implementing the NCIJTF as outlined in the March 2008 Office of Director of National Intelligence report on CNCI implementation. As described in Appendix VII, we analyzed the documentation that the FBI provided to us in January 2011 and consider it to sufficiently evidence FBI actions necessary to close Recommendation 1 of this report.

EXHIBIT 1-1
SUMMARY OF FBI PROGRESS TOWARD COMPLETING CNCI DEVELOPMENT MILESTONES FOR THE NCIJTF[30]

Milestone Dates and Associated Tasks	Completed as of March 2010	Completed as of October 2010
December 2007		
Establish NCIJTF operational framework.	√	
Create FBI National Security Cyber Unit.	√	
Acquire initial NCIJTF work space.	√	
[redacted]	√	
Draft Memoranda of Understanding (MOU).	√	
June 2008		
Draft initial Attorney General guidelines for NCIJTF.	√	
Develop an Attorney General operational plan for NCIJTF.	√	
Complete a plan for coordination and application of law enforcement capabilities to better support investigations of cyber incidents.	√	
Identify requirements for long term NCIJTF facility.	√	
Increase staffing to FBI Headquarters and field office to support cyber security initiatives.	√	
Realign and reprioritize FBI investigative priorities to support cyber security initiatives directly.	√	
Draft procedures and format for joint products and begin to produce intelligence reports.	√	
[redacted]	√	
Fully integrate intelligence community members into the NCIJTF.	√	

[30] This table reflects the NCIJTF development milestones in the FBI's CNCI 2nd Quarter 2009 and 4th Quarter 2010 Quarterly Reports, which the FBI used to report to the Office of the Director of National Intelligence on the execution of FBI activities funded through the CNCI.

Milestone Dates and Associated Tasks	Completed as of March 2010	Completed as of October 2010
March 2009		
Provide initial operational capability to detect, predict, and disrupt intrusions and attacks on U.S. cyber infrastructure.	√	
Identify requirements and request funding to establish a 24/7 joint operations center and long term NCIJTF facilities.	√	
Establish a mature NCIJTF with fully integrated role, mission, and operations.	√	
[redacted]	√	
Establish procedures and format for joint products and begin to produce intelligence reports.	√	
Expand deconfliction of investigations and operations among joint partners.	√	
Obtain approval of MOUs between agencies to establish working and collaboration procedures.	√	
September 2010		
Ensure NCIJTF functions as a multi-agency national focal point for coordinating, deconflicting, integrating, and sharing intelligence regarding all federal domestic cyber threat investigations.	√	
Review and improve procedures and format for joint products and continue to produce intelligence reports.		√
[redacted]		√
Establish a mature process to deconflict investigations and operations among joint partners.		√
Increase proactive investigations and case initiations.	√	
Ensure strategic management of proactive operations and investigations.	√	

Source: National Cyber Investigative Joint Task Force

Information Sharing

By using investigative, technical, counterterrorism, and counterintelligence expertise from agencies across the U.S. government, the

NCIJTF offers a valuable framework for determining who is attacking computer networks and identifying what information the attackers are seeking. In this effort, it is vital that the NCIJTF and its partners have implemented clear policies for information sharing. While the NCIJTF has begun to make strides toward meeting this goal, it faces continued challenges in this area.

According to the NCIJTF Operational Plan, the information sharing methodology at the NCIJTF is intended to provide a "safe harbor" for information that preserves the sources, methods, and authorities of participating agencies. Within this information sharing framework, NCIJTF partner agencies that originate information used by the NCIJTF are to retain dissemination authority for its information. Therefore, the member agency that collects a piece of intelligence is to be consulted before another member agency can act on or further disseminate that information. However, the FBI has encountered challenges in getting NCIJTF partners to agree to this proposed information sharing methodology.

One of the primary findings of the 9/11 Commission was that information sharing among U.S. intelligence and law enforcement agencies was inadequate and that these agencies needed to shift from a need-to-know information sharing model to a need-to-share model.[31] The NCIJTF was intended to promote interagency access to and sharing of information about cyber threats. However, we found that task force members, including the FBI, first attempted to determine the relevancy and importance of its information to another agency's operations before sharing that information with another agency. FBI Cyber Division officials stated that Presidential Directive NSPD-54/HSPD-23 does not give the FBI Director authority to require its NCIJTF partners to share information. These officials stated that any limitations on the sharing of information at the NCIJTF were probably the result of legal restrictions and statutorily-defined jurisdictions.

For example, a Naval Criminal Investigative Service (NCIS) representative to the NCIJTF told us that during an NCIS investigation of an intrusion [redacted], the NCIS found that a hacker was using a compromised computer network within the [redacted] geographic area of responsibility. The NCIS shared the information with the FBI and asked the FBI to report the results of its investigation to the NCIS so that the NCIS could further analyze the threat [redacted]. However, the NCIS representative told us in May 2009 that the FBI had neither provided the information requested about the investigation or a reason for

[31] National Commission on Terrorist Attacks, The 9/11 Commission Report: Final Report of the National Commission on Terrorists Attacks Upon the United States.

not providing the information. The FBI provided us documentation showing that in November 2009 the NCIS was given access to the aforementioned information.

A representative from Air Force Office of Special Investigations told us that the level of FBI information sharing depends on the individual FBI official to whom he directs his request. Air Force Office of Special Investigations headquarters stated that information sharing was routine and productive, but that it would welcome discussions of a more formalized structure to strengthen the processes through which information is shared.

As partner agencies are denied access to information, it also diminishes their knowledge of ongoing threats which can impede the ability of the U.S. government to connect intelligence and determine the origin of future threats.

Threat Focus Cells

A threat focus cell is a team of personnel focused on a specific set of intrusions that share a common actor, method, or target. Threat focus cells include members from participating agencies that can provide the skills and expertise needed to address a particular threat. Each threat focus cell may include agents, intelligence analysts, technical analysts, and engineers specializing in analytical and visualization tools. The FBI instituted the use of threat focus cells at the NCIJTF to better analyze cyber intrusions and attacks against U.S infrastructure. [redacted]

NCIJTF representatives told us that most information sharing within the NCIJTF occurs during threat focus cell meetings. Sharing information during threat focus cell meetings [redacted]

According to an NCIJTF representative and an FBI field agent, some agencies are often asked to leave threat focus cell meetings when information is being shared, since the policy of need to know is enforced. According to the full-time NSA representative on the NCIJTF, [redacted]. Yet, as discussed later in this report, the participation of the NSA, [redacted] The NSA stated that although its representative to the NCIJTF [redacted], other NSA personnel occasionally represented the agency at these meetings.

In response to a draft of this report, FBI officials said it is not the NCIJTF's practice to invite members to threat focus cell meetings. The FBI stated that threat focus cell meetings are posted on a display in the entryway and announced at weekly or biweekly NCIJTF-wide meetings.

Memorandum of Understanding

The NCIJTF Operational Plan calls for each NCIJTF partner agency to sign a memorandum of understanding (MOU) stating that it agrees to share information according to the tenets in the NCIJTF Operational Plan. The MOU outlines how signatory agencies will share information with other partners at the NCIJTF.

As of June 2010, 12 of the 18 member agencies had signed the NCIJTF MOU – all four CNCI-required NCIJTF member agencies – the FBI, [redacted] NSA, and U.S. Secret Service – as well as the Air Force Office of Special Investigation, the Defense Security Service, Naval Criminal Investigative Service, Department of Energy, Department of State, Joint Task Force – Global Network Operations, National Geospatial Intelligence Agency, and Department of Homeland Security – U.S. Computer Emergency Readiness Team (US-CERT). Other partner agencies were not willing to sign an MOU.[32] The Department of Justice (Department), although a participating agency at the NCIJTF, has not signed an MOU. According to the Department's liaison to the NCIJTF, the Department is not required to sign an MOU because the Department does not have personnel assigned to work at the NCIJTF. Instead, the Department's role at the NCIJTF is that of legal consultant and does not participate in the day-to-day operations of the NCIJTF.

We also found that the information sharing requirements in the signed MOUs did not conform to the information sharing framework described in the NCIJTF Operational Plan. The NCIJTF Operational Plan called for partner agencies to share all information legally available but to also retain the right to decide when information could be disseminated outside of the NCIJTF.

[32] The following six agencies that participate at the NCIJTF have not signed an MOU: Department of Justice, U.S. Army 902nd Military Intelligence Group, U.S. Army Intelligence and Security Command, Defense Intelligence Agency, U.S. Army Criminal Investigative Division, and Defense Criminal Investigative Service.

We reviewed the five signed MOUs and, according to the MOUs, agencies control what information will be shared within the NCIJTF, as well as outside the task force.

Additionally, the FBI limits access to certain information to agencies that signed an MOU. For example, the NCIJTF maintains a repository of raw intelligence that comes into the NCIJTF through the partner agencies. In May 2009, according to the Naval Criminal Investigative Service (NCIS) representative to the NCIJTF, the NCIS did not have access to the information contained in the repository because the NCIS had not signed the MOU. Since this time the NCIS signed the MOU, and the FBI provided us documentation demonstrating that the NCIS was given access to the repository.

Without signed MOUs, the NCIJTF partners do not have an adequate understanding of why some information is shared and why other information is not. This has caused some NCIJTF agencies to become concerned about information sharing within the task force and has affected the level of collaboration at the NCIJTF.

According to the FBI Cyber Division Deputy Assistant Director, some participating agencies do not want to, or cannot, share all information with all of the NCIJTF partners due to legal constraints and their agency's policies. He said that because the FBI is the lead agency, those NCIJTF personnel often inaccurately attribute to the FBI the decisions by any NCIJTF agency to not share information.

Integrating the Intelligence Community

The CNCI states that combating the cyber threat must be done in a collaborative manner involving government agencies and the private sector. To that end, the Directive requires the FBI, [redacted] NSA, and U.S. Secret Service to participate at the NCIJTF. The FBI has also invited 10 other agencies named in Executive Order 12333, which outlines the agencies responsible for United States intelligence activities, to join the NCIJTF.[33]

Until July 2009, of the four agencies named in Presidential Directive NSPD-54/HSPD-23 to provide representatives to the NCIJTF, the FBI, U.S. Secret Service, [redacted] had assigned permanent cyber personnel for day-to-day operations of the NCIJTF. The NSA did not commit permanent representatives to work at the NCIJTF until July 2009 – 18 months after the task force was established. [redacted]

[33] Appendix IV lists the agencies named in Executive Order 12333.

[redacted]

[redacted] With this capability and authority, it is critical that the NSA is fully integrated into the NCIJTF. However, as we discussed previously, we found that even after the NSA assigned permanent representation to the NCIJTF, the NSA representative was not fully integrated into the operations of the NCIJTF. In our opinion, the FBI must ensure that the NSA is included in daily NCIJTF operations, incorporated in threat focus cell meetings, and granted access to NCIJTF intelligence.

The Acting Assistant Director of the Cyber Division agreed that the NSA was not fully integrated into the NCIJTF. He said that the NSA had assigned a person from the NSA/Central Security Service Threat Operations Center (NTOC), which monitors the operations of the global network to [redacted]. However, he believed that it would be beneficial to the NCIJTF for the NSA to assign a representative from its [redacted]. In response to a draft of this report, the FBI stated that the NSA has assigned to the NCIJTF a representative from [redacted]. The NSA stated that it had originally embedded only the NTOC into the NCIJTF because it wanted the NCIJTF to work through the NTOC for all NSA support.

NCIJTF Coordination with FBI Field Offices

The NCIJTF Operational Plan states that the success of NCIJTF operations is heavily dependent on FBI field office investigations. FBI field offices are supposed to provide the NCIJTF information obtained during their national security cyber investigations. Likewise, according to the CNCI report, appropriate information from NCIJTF operations should be reported to the field offices to aid in ongoing and future investigations.

We visited 10 FBI field offices and interviewed agents specifically tasked with performing cyber-related investigations with a particular emphasis on national security intrusions. Although the NCIJTF is the centerpiece of the FBI's national security cyber intrusion operations, we found that approximately 36 percent of the 36 FBI cyber agents we interviewed had not heard of the NCIJTF. Although agents are aware of the FBI's Cyber National Security Section, which leads and is located within the

NCIJTF, we are concerned that the cyber field agents we interviewed did not know of the NCIJTF and its mission. We believe this may cause agents in the field to not understand the impact their casework may have beyond the FBI – on government-wide operations being coordinated through the NCIJTF. As a result, agents may not communicate case information as timely or as effectively as needed.

NCIJTF Support of Field Offices

The Cyber Division's Cyber National Security Section program managers, who are located at the NCIJTF, are responsible for coordinating FBI investigations on a national level and ensuring that FBI field agents have sufficient information related to their cyber investigations. These program managers are important to all stages of national security cyber intrusion investigations because they can identify trends, perform deconfliction, help ensure coordination, and provide other valuable information to field offices.

However, the five program managers we interviewed said they could not sufficiently coordinate with FBI field offices because of the demands of their workload. These program managers stated that they did not have the time to return all phone calls that they received from the field offices and that they were not able to disseminate to field offices all the intelligence acquired at the NCIJTF that is relevant to cases being investigated by field offices. The program managers said they instead have to spend more time communicating with agents working investigations that are more developed and closer to identifying persons or governments responsible for attacking the nations' networks. However, the program managers acknowledged that this prioritization did not necessarily mean that lower priority cases were less significant, only that they were less developed. Also, program managers said that a significant part of their job is to create a comprehensive site picture of various cyber threat actors. Program managers said that critical intelligence from lower priority investigations may be overlooked due to their workload.

Because the FBI is the lead agency at the NCIJTF, it has co-located the National Security Cyber Section and the NCIJTF. As a result of this co-location, the section's program managers have assumed dual responsibilities – providing support to the field offices and representing the FBI during NCIJTF threat focus cell meetings. According to the program managers and NCIJTF partner agency representatives that we interviewed, however, FBI program managers are overwhelmed with the breadth and requirements of their responsibilities.

NCIJTF Actions to Address Operational Challenges

In June 2009, the NCIJTF held an off-site meeting with all NCIJTF partners to discuss operational challenges. The off-site meeting produced several recommendations to improve the NCIJTF. Exhibit 1-2 highlights the recommendations related to our findings.

EXHIBIT 1-2
NCIJTF June 2009 Off-site Meeting
Subset of Recommendations

Topic Area	Recommendation
Information Sharing	*Creating member agency transparency by developing technical solutions to foster better collaboration and information sharing.* As of April 2010, the FBI had developed a repository for housing intelligence gathered by each agency. However, guidance on how agencies would collaborate on the information contained in the repository was not established.
	Identifying and eliminating knowledge gaps among participating member agencies by establishing methods for capturing and sharing information. According to the FBI, it has established Threat Focus Cells as a forum for sharing information; all information sharing requests would be initiated through the Threat Focus Cells.
Integrating the Intelligence Community	*Defining member agencies' roles and responsibilities to determine minimum participation levels including attendance requirements to threat focus cell meetings.* According to the FBI, as of April 2010, it had drafted the NCIJTF Operating Instruction that establishes policy, assigns responsibilities, and prescribes standard operating procedures for the task force. The FBI submitted the document to the other participating agencies for comment.
Field Office Support	*Advancing cyber threat investigations by defining strategic and tactical analytical intelligence requirements, necessary skill set for analytical personnel, and analyst training and development requirements.* According to the FBI, its job descriptions identify the required cyber skill set and the Cyber Division's Cyber Education and Development Unit provides FBI cyber agents with cyber training. However, in reference to defining strategic and tactical analytical intelligence requirements, the FBI stated that it has conducted preliminary research but no formal products have been created.

Source: National Cyber Investigative Joint Task Force

Although the FBI formed working groups to implement these recommendations, as of April 2010 the recommendations had not been fully implemented. According to officials from both the FBI and its NCIJTF partners, because the NCIJTF's operational demands are so great, the challenge to adopting some recommendations has been finding the time to devote to their implementation. Many recommendations mirror what we have found during our audit, and we believe that the FBI should work to ensure their implementation.

NCIJTF Operational Successes

According to the CNCI report, the success of the NCIJTF is measured by the number of: [redacted].[34] Exhibit 1-3 shows the NCIJTF performance targets and actual accomplishments for FY 2009 and through the 2nd quarter of FY 2010.

[34] In response to a draft of this report, the FBI stated that it has discontinued using the number of [redacted] as a performance target for FY 2011. The FBI also told us that its Office of General Counsel issued revised guidance in the third quarter of FY 2009 for determining when an investigative operation is considered [redacted] Many activities previously reported as [redacted] no longer meet the FBI's new criteria. The FBI stated that much of this change in interpretation is the result of an evolving understanding of the modes of [redacted].

EXHIBIT 1-3
NCIJTF Performance Targets and Accomplishments
Fiscal Years 2009 and 2010 (as of March 2010)

Performance Criteria	FY 2009		FY 2010	
	Annual Target	Annual Actual	Annual Target	Actual thru 2nd Quarter
[redacted]				

Source: National Cyber Investigative Joint Task Force

[35] The number [redacted].

[36] The number of [redacted] does not include [redacted] created at the NCIJTF; instead, it includes [redacted] produced by the FBI using disseminable, FBI-collected information.

[37] The number of [redacted] does not include [redacted] created at the NCIJTF; instead it includes [redacted] produced by individual agencies based on the information obtained from the NCIJTF collaboration.

As shown in Exhibit 1-3, the NCIJTF exceeded many of its target performance measures. Additionally, during its first 18 months of operation the NCIJTF [redacted].[38] [redacted]

[redacted]

[redacted]

Recommendations

We recommend that the FBI:

1. Ensure the completion of the activities for implementing the NCIJTF as outlined in the March 2008 Office of Director of National Intelligence report on CNCI implementation.

2. Establish policies and procedures, agreed to by NCIJTF partners, for the sharing of information within the NCIJTF.

3. Continue efforts to obtain signed Memoranda of Understanding from the NCIJTF's participating agencies.

[38] The specific details of the successful operations are classified at a higher level than this report and as such are not included.

4. Enhance efforts to educate FBI field office personnel on the NCIJTF's role and use within FBI's national security cyber strategy.

5. Ensure Cyber National Security Section program managers provide cyber agents in field offices with the operational guidance and casework coordination necessary to fully investigate national security intrusion cases effectively.

Finding II: Field Office Capability to Investigate National Security Cyber Intrusion Cases

> In the FBI field offices we visited, we found that 64 percent of the FBI cyber agents we interviewed assigned to national security cyber intrusion cases had the technical skills that Cyber Division officials believed was needed to investigate these types of cases. The other 36 percent of agents we interviewed lacked the necessary information technology knowledge expertise to effectively investigate national security intrusion cases. Further, some FBI agents assigned to investigate national security cyber intrusion cases told us that they did not feel qualified to investigate national security intrusions effectively. We also found that the forensic and analytical capability in the field offices was inadequate to fully support field offices' national security intrusion investigations. In addition, we found that the staged format of the FBI's cyber development plan can impede an agent's ability to acquire the training needed to investigate national security intrusion cases effectively. Finally, we believe that the FBI's rotation policy and resource allocation strategy hinder some FBI field offices' ability to effectively investigate national security intrusion cases.

As with other types of investigations, FBI field offices are the primary component of the FBI's efforts to address national security cyber intrusions. In national security intrusion investigations, it is important for field offices' cyber agents to understand current techniques and tactics used by those engaged in illicit cyber activities. In addition, these agents must keep abreast of emerging technologies that are used to overcome computer systems' defenses and to infiltrate networks, such as those of the U.S. government, utility companies, defense contractors, and financial institutions.

FBI Cyber Career Path

In 2007, the FBI developed career paths that emphasize training and experience in five areas: criminal investigation, intelligence, counterterrorism, counterintelligence, and cyber matters. The FBI believes these career paths build expertise, both at an individual and organizational level, in the five critical areas.

According to FBI data, of the 13,492 special agents the FBI employed as of March 2010, [redacted] were designated as cyber agents through the FBI Special Agent Career Path (Career Path) program.

Cyber Development Plan

In January 2007, as part of the implementation of the cyber career path, the FBI established a developmental plan within the Cyber Career Path. The Cyber Development Plan, as shown in Exhibit 2-1, is divided into four stages based on the number of years an agent is part of the cyber career path program. Each stage requires agents to complete specific training courses and have experience with FBI procedures and investigative techniques. The development plan includes 12 core courses that each agent must complete, as well as optional courses with a more specialized focus. The FBI stated that it expects agents to complete the 12 core courses and on the job training required by the development plan in 5 to 7 years.

EXHIBIT 2-1
OVERVIEW OF THE CYBER DEVELOPMENT PLAN

Stage	Level	Core Courses	On-the-Job Training
One	New Agent Training	General courses applicable to all career paths	Not Applicable
Two	New Agent Training to 3 Years	Post New Agent Training A+ Certification Linux for Law Enforcement Introduction to Counterintelligence/ Counterterrorism Investigations Operating Systems	Understanding of the Cyber mission Working knowledge of all cyber-related investigations Detailed knowledge of the written requirements for initiation, conduct, reporting, and resolution/termination of basic cyber investigations and informant matters
Three	3 to 5 years	Network Investigation Techniques for Agents Network + Certification Wireless Technology SANS Security 401: Security Essentials Bootcamp Style	Familiarity with written requirements for Foreign Intelligence Surveillance Act requests and/or renewals and for obtaining and issuing National Security Letters Working knowledge of how to read, understand, and interpret an Intelligence Information Report (IIR) Learn legal criteria and guidelines for the employment of investigative cyber tools Make at least one cyber-related presentation to an outside group Working knowledge of reporting, disseminating, and sharing investigative findings
Four	More than 5 years	Advanced Network Investigation – Unix and Windows (separate courses) Network Traffic Analysis Intrusion Response	Initiate and successfully prosecute a major case Case agent for a computer Title III investigation Ability to configure an UNIX kernel and in-depth knowledge of the Windows Registry

Source: FBI Cyber Division's Education and Development Unit

The FBI considers agents who complete the core courses of the development plan to be quality cyber agents, but we found that as of June 2010, only [redacted] cyber agents had completed or tested out of all 12 core courses of the development plan. While many of the agents we interviewed said the training required by the development plan was helpful, they also said they did not have the time to take the required courses.

According to the Cyber development plan, until agents have completed stage two of the development plan they are not permitted to take courses covering network traffic analysis, advanced network investigation techniques, network log analysis, and systems forensics. However, these courses were said to be extremely beneficial to agents in developing the skills necessary to investigate national security intrusions. Many field agents we interviewed said agents who do not have prior networking experience cannot adequately investigate national security intrusion cases. As a result, the staged format of the development plan can impede an agent's ability to acquire the training necessary to investigate national security intrusion cases effectively. In its response to a draft of this report, the FBI said that it has allowed agents to bypass prerequisite courses when more advance classes are pertinent to their current case assignments.

Many agents said that the development plan was incomplete because it did not include a step-by-step course on how to investigate national security intrusion cases. However, the FBI's New Agent Training program does include a course instructing participants on how to investigate cyber intrusion cases. Given that agents do not recall this instruction, we believe the FBI should evaluate the effectiveness of this cyber intrusion course.

Moreover, because the FBI requires new agents assigned to [redacted] offices to transfer to another office after 3 years, we found that the 5-year development plan is particularly problematic for [redacted]. Based on the FBI criteria for a quality cyber investigator, newly-hired cyber agents may not be considered qualified to investigate national security cyber intrusion cases. New agents [redacted] are also less likely to receive the benefit of on-the-job training and mentorship from more experienced and qualified cyber agents, which is a major element of the FBI's cyber agent development plan. According to the FBI's response to our draft report, its staffing goal [redacted] is that no more than 20 percent of each field office's agents have less than 3 years of experience. We found that, in FY 2009, 35 percent of the cyber agents in [redacted] had less than 3 years experience.

In the [redacted], the 5-year timeframe outlined in the developmental plan is less problematic for training new agents to investigate national security intrusions. New agents who are [redacted] not subject to the FBI's rotation policy. In addition, [redacted] relying less on classroom training to develop new agents.

Intrusion Specialty

FBI officials stated that the successful investigation of cyber intrusions requires agents to have a higher technical capability than agents investigating other cyber matters, such as on-line child pornography, and intellectual property rights. Yet, the cyber agent career path does not have any specialty areas, such as an intrusion specialty, to better ensure the development of more skilled agents to investigate the more technical cyber matters.

Two Cyber Division unit chiefs we interviewed advocated the creation of an "intrusion specialist" within the cyber agent career path. The two unit chiefs believed that an intrusion specialist should be certified in computer operations and network infrastructure, including A+ and Network+ certifications.[39] In addition, the two unit chiefs believe that an intrusion specialist should be able to: (1) understand Microsoft Windows and Linux operating system registries to determine the effects of malicious codes and the types of logs created by both operating systems, (2) understand how networking devices communicate with each other, (3) check network logs to uncover anomalies in application, and (4) analyze raw network traffic and system application logs.[40] Given the highly technical and evolving aspects of cyber intrusion cases, we agree that it would be beneficial for the Cyber Division to develop an intrusion specialty within the Cyber Career Path.

To assess the qualifications of current cyber agents to investigate cyber intrusion matters, we examined whether the 36 cyber agents we

[39] The A+ certification demonstrates the agent's competency as a computer technician while the Network+ certification demonstrated the agent's competency in managing, maintaining, troubleshooting, installing, and configuring a basic networking infrastructure.

[40] The listed skills and abilities can be gained from working in the IT systems networking field, for example, as a system network administrator.

interviewed had the above-listed capabilities as described by the Cyber Division Unit Chiefs. We found that 23 (64 percent) of these agents reported they had the intrusion specialist capabilities described above. Therefore, 13 (36 percent) of the agents we interviewed who were responsible for investigating national security intrusion matters reported that they did not have this skill set.

In our assessment of cyber agent qualifications, we also examined each agent's prior work experience and formal education. We determined that only 50 percent of the agents we interviewed who were investigating national security intrusion matters had prior work experience in an information technology-related field.[41]

We believe the development of an intrusion specialty within the cyber career path would better enable the FBI to hire and train qualified personnel to investigate intrusion matters effectively. As part of the specialty, the FBI should identify any prerequisite or optimal qualifications for agents to being admitted into the specialized career path and create a training curriculum that includes courses on information technology and investigative techniques critical to investigating cyber intrusion cases successfully.

Field Office National Security Cyber Intrusion Efforts

The 10 FBI field offices we visited included small, medium, and large offices with varying numbers of national security intrusion cases.[42] We interviewed a total of 36 agents who were assigned to investigate national security intrusions and assessed their qualifications to conduct this type of specialized cyber investigation. Additionally, we examined the number of active cases and the level of effort expended on investigating these cases.

Field Qualifications

As shown in Exhibit 2-2, we compared the technical skill set of the 36 national security intrusion agents we interviewed by examining their prior work experience, formal education, and training. Specifically, we determined whether agents had prior work experience in network

[41] The other degrees included accounting, engineering and mathematics, law, politics, criminal justice, sociology, and psychology.

[42] Please see Appendix I for a detailed description of the methodology we used to select the 10 field offices. The 10 field offices we visited were [redacted].

administration, earned an information technology degree, and completed the core courses of the cyber development plan. As noted previously, [redacted] of FBI's cyber agents had completed or tested out of the Cyber Career Path developmental core courses as of June 2010. Additionally, we found that while 18 of the 36 agents interviewed had degrees in information technology, only 8 of the agents had prior experience in network administration. Several agents told us that not all information technology degrees necessarily provide the skills required to investigate national security intrusion cases.

EXHIBIT 2-2
EXPERIENCE AND TRAINING OF 36 CYBER AGENTS INTERVIEWED WHO WERE ASSIGNED TO INVESTIGATE NATIONAL SECURITY CYBER INTRUSIONS AT THE 10 OFFICES WE VISITED

	National Security Intrusion Agents Interviewed	Prior Network Administration Work Experience	Information Technology Degree	Completed 12 Core Courses	Average Core Courses Completed (per Agent)
[redacted]	3	2	2	0	6.66
[redacted]	7	1	3	1	6.92
[redacted]	6	1	3	0	6.00
[redacted]	2	1	2	1	6.66
[redacted]	4	0	1	0	5.80
[redacted]	4	1	1	0	4.48
[redacted]	2	0	1	0	3.33
[redacted]	2	0	2	0	2.42
[redacted]	2	1	2	0	4.66
[redacted]	4	1	1	0	5.00
TOTAL	36	8	18	2	5.19

Source: Federal Bureau of Investigation

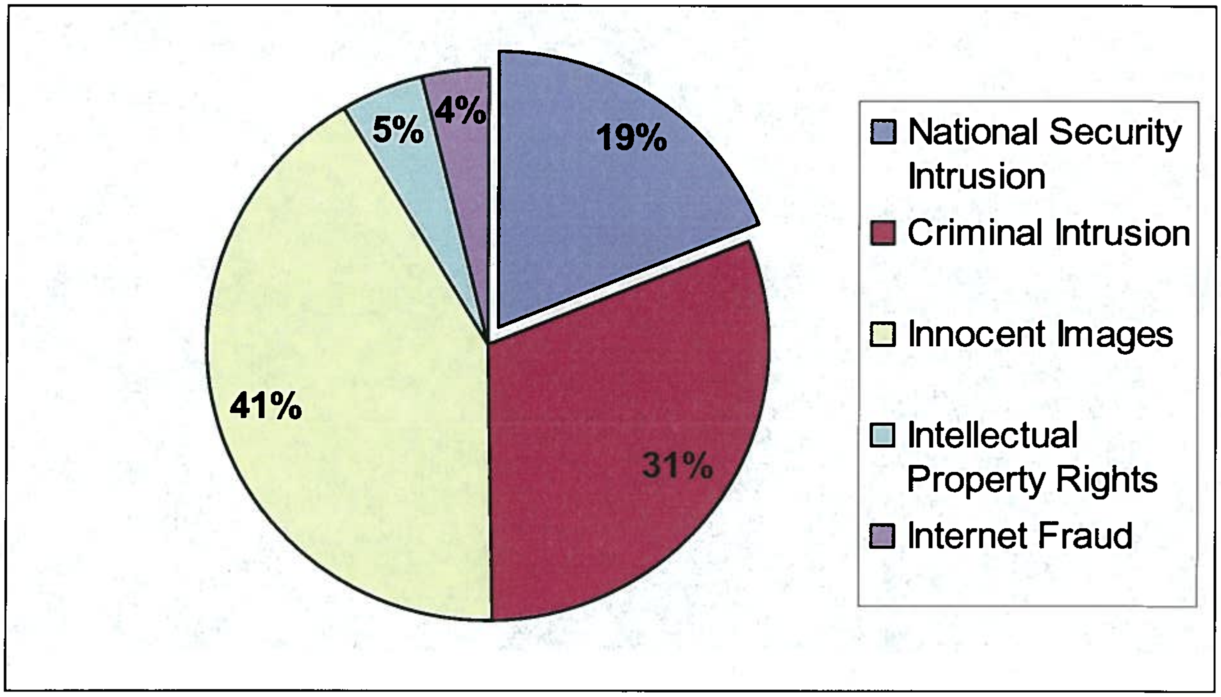
Field Efforts

NCIJTF personnel stated that there are more national security intrusions, the FBI's top cyber priority, than the FBI can address. However, the FBI does not centrally track the number of intrusions that it is not able to address. Thus, without a review of all complaint files, the FBI cannot determine the total number of intrusions that the FBI does not address.

As shown in Exhibit 2-3, in FY 2009 the FBI used 19 percent of its cyber agents on national security intrusion investigations. The FBI used

41 percent of its cyber agents to investigate online child pornography matters.

EXHIBIT 2-3
UTILIZATION OF AGENTS ON CYBER INVESTIGATIONS[43]



Source: Federal Bureau of Investigation

In FY 2009, the FBI allocated [redacted] special agents to investigate all types of cyber cases in the 10 field offices we visited. These 10 offices assigned [redacted] agents (37 percent of the [redacted] allocated to investigate all types of cyber cases) to investigate national security intrusion cases.[44] However, as of September 2009 only [redacted] agents from these field offices – or 45 percent of the [redacted] agents assigned – reported that they actually worked on national security cases.

[43] According to Cyber Division guidance on conducting and classifying cyber investigations, a national security intrusion is one conducted for intelligence or terrorist purposes by foreign powers, including international terrorist groups. Criminal intrusions are those motivated for criminal conduct.

[44] These assigned agents sometimes include non-cyber career path agents that field offices assign to cyber squads, such as agents allocated to counterterrorism and counterintelligence programs. For instance, [redacted] field offices each assigned two non-cyber agents to cyber squads.

EXHIBIT 2-4
FBI FIELD OFFICE SPECIAL AGENTS
IN 10 FIELD OFFICES VISITED
ALLOCATED POSITIONS VERSUS ACTUAL AGENT UTILIZATION
FISCAL YEAR 2009

[redacted]

Source: Federal Bureau of Investigation

In our interviews with the 36 field agents, five stated that they did not feel qualified to investigate national security intrusions and were not able to investigate these matters effectively. For example, one agent told us that he was assigned his first counterterrorism intrusion case but he did not know how to investigate a national security intrusion case and was concerned about his ability to perform the investigation.

The Assistant Director for the Cyber Division acknowledged that not every field office has the expertise to adequately investigate every national security intrusion it encountered. He said the Cyber Division plans to build a base capability in every field office and, when needed, supplement that capability with resources from field offices with larger more experienced cyber squads. He said this plan was in its infancy, and the Cyber Division had not yet determined what constitutes a base capability and which offices would provide the supplemental resources.

Additionally, Field offices Special Agents in Charge have the discretion to utilize agents outside their career path. During our visits to the 10 FBI field offices, we found that cyber agents were often being used in other investigations instead of on cyber-related matters, such as counterintelligence, white collar crimes, and violent crimes cases.

Allocation of Resources

The Cyber Division's investigative priorities are: (1) computer intrusions, (2) child sexual exploitation, (3) intellectual property rights, and (4) internet fraud.[45] According to the Cyber Division's Deputy Assistant Director, the Cyber Division allocates personnel to the field offices based on the number of priority cyber cases being investigated by the field office. However, the Cyber Division did not determine cyber threats within the field offices' jurisdiction or overall cyber resource needs. As a result, field offices with a significant national security intrusion threat may not have the resources to address this high priority area effectively. The FBI stated that it uses Regional Cyber Action Teams (RCAT) to provide additional resources to high-priority cases, when needed.[46]

For example, we found that the [redacted] did not open a national security intrusion case in FYs 2007 and 2008. In accordance with the Cyber Division's policy of allocating cyber agents to field offices based on their level of activity in national security intrusions, the [redacted] not receive additional cyber agents during these two fiscal years. The Cyber Division did not inquire as to why [redacted] had not opened any national security intrusion cases during that time. The Assistant Special Agent in Charge (ASAC) of the [redacted] told us that the office was not opening national security intrusion cases because the office did not have agents who were qualified to investigate this type of case. Because of its lack of agents qualified to investigate national security intrusions, the field office was not able to determine when thousands of intrusions in its area of responsibility began or what information the intruders took.

An April 2010 OIG audit report found that the FBI was in the process of implementing throughout its programs a risk-based resource management model that would identify risk indicators affecting field offices

[45] Counterterrorism and counterintelligence intrusions are the primary focus of the Cyber Division's computer intrusion efforts because of their relationship to national security matters. Criminal intrusions then follow in priority. This audit focuses on the FBI's efforts in investigating counterterrorism and counterintelligence computer intrusion cases.

[46] Regional Cyber Action Teams (RCAT) are deployed globally at the direction of FBI Cyber Division executive management. According to the FBI, RCATs bring in-depth cyber expertise, specialized investigative skills, and direct connectivity to cyber initiatives, investigations, and emergencies.

and allocate agent positions to field offices based in part on those indicators.[47] The OIG report specifically recommended that the FBI require the Cyber Division to utilize a more sophisticated resource allocation methodology, such as the FBI's risk-based management model. In April 2010, the Cyber Division stated that it had started to implement this risk-based allocation model. The Cyber Division also stated that it was working to better account for the non-geographic nature of cyber crimes in its model.

Rotation Policy

In July 2005, the FBI Director approved the First Office Agent Rotational Transfer Policy (rotation policy).[48] In the memorandum announcing this policy the FBI Director stated that this rotation policy was intended to ensure structured progression from broad-based field experience, frequently found in small to medium size offices, to more specialized experience in handling complex investigations and intelligence responsibilities, frequently found in large field offices.[49]

The rotation policy calls for new agents [redacted] based on the current staffing level of the office or critical, specialty needs to rotate [redacted] after 3 years. When an agent rotates [redacted], the agent's cases remain and are reassigned to other agents who are often agents in their first assignments out of the FBI Academy.

According to the rotation policy, the FBI's smaller field offices offer agents an opportunity to learn how to conduct investigations of cases on a smaller scale and with lower level of complexity than typically encountered at the FBI's larger field offices.

However, national security cyber intrusions do not follow this model because national security intrusions are not concentrated in any particular area of the country and do not necessarily vary in complexity depending on the locale. For example, when a foreign country uses computer networks to attack a defense contractor in Memphis, it uses the same

[47] U.S. Department of Justice Office of the Inspector General, *Follow-up Audit of Federal Bureau of Investigation Personnel Resource Management and Casework,* April 2010. Risk indicators highlight the potential for an adverse outcome of threats, vulnerabilities, and consequences associated with events.

[48] In October 2006, the rotation policy was revised to change the definition of a large field office and change the effective rotation date.

[49] For the FBI rotation policy, a field office is considered large if it has a funded staffing level of over 200 agents.

technology and techniques to attack a defense contractor in New York. As a result, the FBI field offices in Memphis and New York need agents equally well-qualified in investigating national security intrusions.

As a result we found that the rotation policy has had significant consequences on the FBI's ability to investigate national security intrusions. [redacted] Because national security intrusion cases are technical and require specific skill set, few new cyber agents can effectively assume responsibility of an open national security intrusion investigation. In 4 of the 10 offices we visited, agents told us they had been assigned cyber cases that exceeded their technical capabilities.

Several agents we interviewed also told us that investigating national security intrusion cases is more complex than investigating other types of cyber crime such as internet fraud, child pornography, and intellectual property rights violations. They stated that national security intrusions require an extensive knowledge of information technology networks and counterintelligence techniques. While most special agents said that classroom instruction is valuable, they emphasized that practical experience was necessary to develop an agent to investigate national security intrusions effectively.

In addition, it is important when investigating national security intrusion cases, like in other high priority cases, for agents to develop partnerships and confidential informants to investigate national security intrusion cases. When an agent rotates to a different field office, the agent normally loses ties with confidential informants and partnerships that were cultivated over the prior three years.

Some of the agents we interviewed during our field office visits were cyber career path agents in their first assignments out of the FBI Academy. These agents had assumed national security intrusion cases from their predecessors who rotated to other field offices. Several said they did not believe that they were prepared to assume the responsibilities of these ongoing cases because they lacked the technical expertise and investigative experience necessary to investigate national security intrusions adequately. These agents told us that they believed the rotation policy further compounded the challenge they faced because experienced cyber agents were often rotated to another office, [redacted]

Effect on Field Offices

[redacted][50]

Based on our review of three agents' technical skill set, training, and experience, we concluded that two of the agents were qualified to conduct national security intrusion investigations. The previous senior cyber agent, whom we found was qualified, rotated to another office in July 2009. According to the Assistant Special Agent in Charge of the [redacted], as of June 2010 the rotated agent was replaced by two agents with excellent cyber backgrounds. He added that since our visit to the field offices, FBI Headquarters has begun to address the shortage of qualified agents in the [redacted] by increasing the number of Personnel Resource List transfers to [redacted].[51]

[redacted] Both employ staff to thwart the thousands of intrusions attempted annually. But the FBI believes that both [redacted] share little information about these attempted intrusions with the FBI because the companies that run them are concerned about the impact the intrusions will have on the [redacted] perception of their ability to provide security. According to the Supervisory Special Agent in the [redacted], the best way for the FBI to obtain valuable data from the intrusions into these facilities is to

[50] [redacted]

[51] The Personnel Resource List is maintained for each field office. Special agents are placed on a field office's Personal Resource List after designating that office as their preferred assigned location.

have experienced agents detailed to these facilities to work with the [redacted] cyber experts.

[redacted]

The same problems from inexperience and frequent rotations can arise in other offices, where agents we interviewed said that a technical background or education cannot be substituted for experience investigating national security intrusions. For example, at the [redacted] we interviewed one of two agents working national security intrusion cases. Even though the agent had degrees in computer science and industrial engineering and worked in an information technology field prior to joining the FBI, this agent told us he was unable to "hit the ground running" when he took over from his predecessor because his extensive information technology experience did not prepare him for investigating national security intrusion cases. He said his degree and experience taught him how to build computers rather than the details of computer security and networking, the skills needed for working national security intrusion cases. He said the national security intrusions were unique because it takes longer than the three-year rotation to develop productive relationships and contacts within the cyber community. He also said that the frequent rotation of agents diminished the FBI's credibility within the cyber community when the positions are backfilled with inexperienced personnel. The [redacted] squad supervisor told us that when a source is handed off to a new agent the source may not make the effort to contact the new agent, and a new relationship does not develop or pay dividends.

According to the supervisor of the [redacted], it took one agent two and a half years to get "up to speed" in investigating national security intrusions after arriving to the [redacted]. Now that the agent is proficient, he has developed sources in the community, allowing the field office to proactively notify targets of potential intrusions into their networks. However, this agent was scheduled to rotate out of the [redacted] within three months of our visit, [redacted].

In short, our findings on the impact of the FBI rotation policy are consistent with what the GAO reported in June 2007, in which it found that the FBI rotation policy had a negative effect on the capabilities of the field office cyber squads.[52] GAO found that the available pool of experienced cyber crime investigators is affected by the FBI's rotation policy. According to the GAO report, when cyber crime investigators rotate from their offices according to the FBI's rotation policy, they are not necessarily reassigned to cyber crime investigations in the new field office, and so their cyber background is underutilized. In addition, the agents who rotate in to replace experienced cyber crime investigators may have little or no cyber crime experience or background.

The GAO recommended that the FBI assess the impact of its current rotation policy on its cyber mission and modify it if necessary. In response, the FBI stated that the Cyber Career Path ensured that the FBI recruits, trains, and deploys special agents with the critical cyber skill set required to keep the FBI on the cutting edge of computer technology and development, and positioned to counter the constantly evolving cyber threat. However, the GAO concluded that the creation of a Cyber Career Path would not be sufficient to ensure that FBI staff with cyber expertise was adequately utilized.

We agree. Because of the specialized nature of the skills needed to effectively investigate national security intrusion cases, we believe the FBI needs to ensure that agents assigned to investigate these cases have the necessary expertise and experience. It is also important for the FBI to ensure that all field offices have access to qualified agents who can effectively investigate national security intrusion cases.

To address the disparity highlighted in the GAO report, the FBI stated that it developed a critical needs transfer program to identify qualified cyber agents to fill cyber vacancies in [redacted] field offices. The FBI stated that in FY 2010 it canvassed its field divisions and [redacted] experienced cyber agents to several of these offices. To be eligible to participate in the transfer program, an agent must have 3 years of experience with cyber investigations; experience as a case

[52] GAO, CYBERCRIME: Public and Private Entities Face Challenges in Addressing Cyber Threats, GAO-07-705 (June 2007).

agent for criminal, counterintelligence and counterterrorism intrusion investigations; and completed stage 3 of the cyber career path required curriculum. The FBI stated that moving more cyber agents to [redacted] offices was planned for November 2010.

Analytical Support

According to a 2004 National Intelligence Council report, the intelligence community can provide long-term strategic warning of the nation's adversaries' technical capabilities and intentions, [redacted] [53] [redacted]

In March 2008, the FBI launched the new Field Intelligence Model, which called for embedding intelligence analysts with FBI operational squads to help ensure the coordination of investigative and intelligence operations.[54] The Field Intelligence Model also stated that intelligence analysts should interpret collection requirements and collaborate with case agents on the collection, filtering, processing, and analysis of information, as well as help develop new confidential sources when existing sources are not providing sufficient intelligence. [redacted] This information is critical to identifying the persons responsible for the intrusions into the nation's networks.

The FBI's Directorate of Intelligence manages the FBI's intelligence program and intelligence analysts. As a result, it is important for the FBI's Cyber Division and Directorate of Intelligence to work together to ensure that field office cyber squads have the tactical analytical support necessary to investigate national security cyber intrusions successfully.

[53] [redacted]

[54] FBI Strategic Execution Team, *The New Field Intelligence Model*, Version 1.0, March 2008 – March 2009.

However, our review determined that FBI field agents are not receiving the tactical analytical support for national security intrusion investigations from intelligence analysts as required by the Field Intelligence Model. According to the intelligence analysts we interviewed, their role is to provide a strategic or overall view, not tactical or case-specific support. Some of the agents we interviewed said that insufficient tactical analytical support hampered their ability to connect the dots in an investigation, further limiting their ability to determine who is responsible for the intrusion.

FBI Response to Field Office Challenges

Since our audit fieldwork, the FBI conducted a review of the Cyber Division Funded Staffing Level (FSL) to address the difficulty that [redacted] field offices experience in maintaining adequate staff in their cyber program. The FBI's review found that [redacted] field offices were allocated more cyber staff than necessary, [redacted] did not have an adequate level of cyber personnel. This internal FBI review attributed to the FBI rotation policy the difficulties of maintaining adequate staffing [redacted].

As a result, the FBI Transfer Unit stated that it was prepared to rotationally transfer cyber-specific agents on a voluntary basis to [redacted]. For the long term, the Cyber Division began realigning its career path program to help ensure [redacted] field offices had qualified agents to investigate national security intrusion matters.[55] As part of redeveloping the cyber career path, the FBI stated that it will remove from the cyber career path agents who do not possess the desired level of cyber skill. FBI field offices must identify agents in the cyber career path who do not possess adequate cyber skills and then give these agents the opportunity to change to a career path more in line with their education, skills, and abilities. Once the Cyber Division completes its realignment, the Transfer Unit will provide voluntary, rotational transfers to [redacted] field offices that are projected to lose cyber agents as a result of the rotation policy.

In addition, the FBI is reducing the number of cyber-track agents in each New Agent Training class by selecting for the cyber career path only agents with significant cyber education or skills. As of April 2010, the Cyber Division's efforts to place qualified agents in [redacted] field offices were still ongoing. According to the Assistant Director

[55] The Cyber Division defines a quality cyber agent as one who have completed the cyber curriculum stages 3 or 4 and who can articulate the ability to competently address all three types of Cyber Division priority cases.

of the Cyber Division, the Cyber Division is in the process of determining what constitutes the base capability for each field office and which offices can afford to transfer qualified cyber special agents to the field offices in need.

Some agents whom we interviewed advocated a regional approach to investigating national security intrusions. These agents argued that the investigations are so specialized that it is unlikely that the FBI will be able to build cyber squads proficient at investigating these cases in every field office. These agents suggested that the FBI create "regional hubs" to investigate national security cases, which would allow the FBI to bring together its best and brightest cyber agents into a small number of national security intrusion squads. These squads would be distributed across the nation and would be responsible for intrusions across a larger territory than the typical size of a field office's territory. Each field office would be able to use the skills and expertise of a regional squad. New agents with the necessary skills could be assigned to a regional hub, where they would learn from experienced agents. We believe the FBI should consider a regional approach to address national security cyber intrusions.

Recommendations

We recommend that the FBI:

6. Evaluate the effectiveness of the step-by-step training course for FBI agents on how to investigate national security intrusion cases.

7. Ensure that cyber career path agents complete the existing curriculum for all stages of the Cyber Development Plan.

8. Reconsider the rotation policy for cyber agents, and ensure that agents skilled and experienced in cyber intrusions are available to FBI field offices.

9. Consider establishing a cyber intrusion specialty within the cyber career path.

10. Consider developing regional hubs with agents expert in investigating national security intrusions.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

As required by the *Government Auditing Standards* we tested, as appropriate given our audit scope and objectives, selected transactions, records, procedures, and practices, to obtain reasonable assurance that FBI's management complied with federal laws and regulations, for which noncompliance, in our judgment, could have a material effect on the results of our audit. FBI's management is responsible for ensuring compliance with applicable federal laws and regulations. In planning our audit, we identified the following laws and regulations that concerned the operations of the FBI and that were significant within the context of the audit objectives:

- Computer Fraud and Abuse Act of 1986;
- Electronic Communications Privacy Act of 1986;
- Economic Espionage Act of 1996;
- USA PATRIOT Act;
- Executive Order 12333 United States Intelligence Activities;
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23;
- Attorney General's Guidelines for Domestic FBI Operations; and

Our audit included examining, on a test basis, FBI's compliance with the aforementioned laws and regulations that could have a material effect on the FBI's operations, through interviewing FBI personnel, analyzing data, examining procedural practices, and assessing internal control procedures. Nothing came to our attention that caused us to believe that the FBI was not in compliance with the aforementioned laws and regulations.

STATEMENT ON INTERNAL CONTROLS

As required by *Government Auditing Standards* we tested, as appropriate, internal controls significant within the context of our audit objectives. A deficiency in an internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to timely prevent or detect: (1) impairments to the effectiveness and efficiency of operations, (2) misstatements in financial or performance information, or (3) violations of laws and regulations. Our evaluation of FBI and NCIJTF internal controls was *not* made for the purpose of providing assurance on its internal control structure as a whole. The FBI's management is responsible for the establishment and maintenance of internal controls.

Through our audit testing, we did not identify any deficiencies in FBI or NCIJTF internal controls that are significant within the context of the audit objectives and based upon the audit work performed that we believe would affect the FBI's ability to effectively and efficiently operate, to correctly state financial and performance information, and to ensure compliance with laws and regulations.

Because we are not expressing an opinion on the FBI's internal control structure as a whole, this statement is intended solely for the information and use of the FBI. This restriction is not intended to limit the distribution of this report, which is a matter of public record. However, we are limiting the distribution of this report because it contains sensitive information that must be controlled appropriately.[56]

[56] A redacted copy of this report, with sensitive information removed, will be made available publicly.

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

The objectives of this audit were to: (1) evaluate FBI efforts to develop and operate the National Cyber Investigative Task Force (NCIJTF) to address the national security cyber threat; and (2) evaluate the FBI's field offices capabilities to investigate national security cyber cases.

Scope and Methodology

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The audit focused on the FBI's efforts to investigate national security intrusion cyber cases.

Our criteria for selecting the 10 field offices included the following criteria:

- special agents transferred due to the 3-year rotation policy;
- national security intrusion investigations opened in FYs 2007 and 2008;
- special agent allocations in FYs 2007 and 2008;
- special agent experience as a percentage of the total allocation;
- special agent hours utilized for national security intrusion investigations;
- special agents that completed the Introduction to Cyber Counterterrorism/Counterintelligence investigations course; and
- special agents that completed Cyber Division courses at the Advanced and Expert level.

We conducted field work at FBI headquarters offices in Washington, D.C., and [redacted], and in the following 10 FBI field offices: [redacted]. We interviewed FBI headquarters personnel, including Cyber Division management, and we interviewed representatives of NCIJTF partners, including the U.S. Army, U.S. Air Force, Department of Energy, Naval Criminal Investigative Service, and U.S. Secret Service.

To evaluate the FBI's development and operation of the NCIJTF, we analyzed the NCIJTF Quarterly Progress Reports to determine if they met the Comprehensive National Cybersecurity Initiative (CNCI) Target Achievements. The CNCI has four set of Target Achievements that are to be completed by December 31, 2007; June 30, 2008; March 31, 2009; and September 30, 2010. The Quarterly Progress Reports provided by the FBI were for FY 2008 and the first 2 quarters of FY 2009, which covers their progress through the March 31, 2009 deadline. We determined whether the FBI accomplished the Target Achievements by matching the FBI's reported accomplishments to the appropriate Target Achievements. Additionally, we interviewed the FBI's NCIJTF partners to evaluate information sharing and collaboration among members of the NCIJTF.

To evaluate the capabilities of the FBI field offices to investigate national security intrusions, we interviewed the FBI Cyber National Security Section program managers and 36 special agents from 10 of the FBI field offices. To evaluate the Cyber National Security Section's roles and functional responsibilities we interviewed Cyber National Security Section program managers to determine their efforts to provide administrative and operational support to national security intrusion investigations and coordination of investigative activity for all field offices.

In assessing the special agents' qualifications for investigating national security cyber intrusions, we considered the agent's: (1) educational background, (2) prior work experience, (3) specific experience working national security intrusions for the FBI, and (4) training and other intrusion specialist skills and abilities. The intrusion specialist skills and abilities included experience in:

- working with [redacted] operating systems,
- using the networking and routing protocols,
- checking logs to test anomalies in application protocols, and

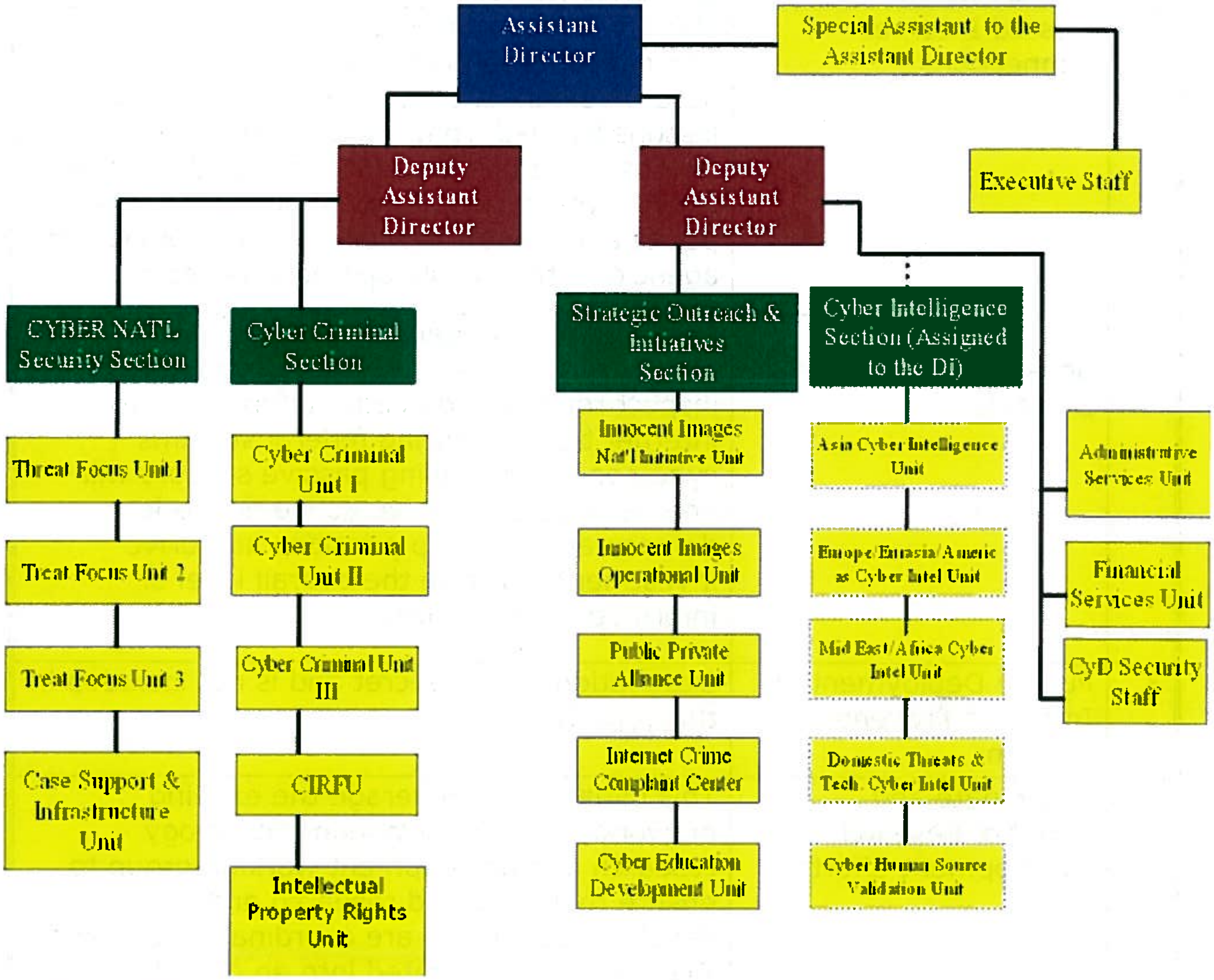
- analyzing raw network traffic and system application logs with analysis tools.

We also assessed the FBI field offices' efforts in investigating counterintelligence and counterterrorism intrusion cases. To accomplish this, we relied on data contained in the FBI's Compass system. Compass is the FBI's central source of real-time information on FBI resources, performance, and accomplishments.

The OIG previously conducted a reliability test on the Compass system on which we relied for this audit. During the previously conducted reliability test, the contractor was unable to sufficiently determine the reliability of Compass data because the FBI did not provide evidence that management reviewed Compass logs and reports. However, the OIG concluded that the results of other Compass testing, along with the results of previous reviews of FBI resource and casework-related data, provided sufficient assurance that the data presented in this report can be used to present and conclude appropriately on FBI resource utilization and caseload.

APPENDIX II

Cyber Division Organization


Assistant Director
Special Assistant to the Assistant Director
Executive Staff
Deputy Assistant Director
Deputy Assistant Director
CYBER NATL Security Section
Threat Focus Unit 1
Treat Focus Unit 2
Treat Focus Unit 3
Case Support & Infrastructure Unit
Cyber Criminal Section
Cyber Criminal Unit I
Cyber Criminal Unit II
Cyber Criminal Unit III
CIRFU
Intellectual Property Rights Unit
Strategic Outreach & Initiatives Section
Innocent Images Nat'l Initiative Unit
Innocent Images Operational Unit
Public Private Alliance Unit
Internet Crime Complaint Center
Cyber Education Development Unit
Cyber Intelligence Section (Assigned to the DI)
Asia Cyber Intelligence Unit
Europe/Eurasia/Americas Cyber Intel Unit
Mid East/Africa Cyber Intel Unit
Domestic Threats & Tech. Cyber Intel Unit
Cyber Human Source Validation Unit
Administrative Services Unit
Financial Services Unit
CyD Security Staff

Source: FBI Cyber Division

APPENDIX III

CNCI INITIATIVES AND STRATEGIC ENABLERS

	INITIATIVE	DESCRIPTION
1	Trusted Internet Connections	This initiative is intended to reduce and consolidate federal government external access points. It takes the best practices and lessons learned from the Department of Defense military network consolidation effort to drive the consolidation of network access points and overall network defense for civilian agencies into a single operations center.
2	Deploy Passive Sensors Across Federal Systems	This initiative is intended to deploy intrusion detection systems using passive sensors to inspect routing and header information for all internet traffic entering federal systems cyberspace. Deploying passive sensors will enable more aggressive active network defense and will help prioritize and drive investments to raise the overall level of information assurance.
3	Pursue Deployment of Intrusion Prevention System	Description is Top Secret and is not included in this report.
4	Coordinate and Redirect Research and Development Efforts	This initiative will leverage the existing networking and information technology research and development working group to ensure that classified research and development efforts are coordinated fully and that they are integrated into an overall plan for cyber research and development.
5	Connect Current Cyber Centers to Enhance Situational Awareness	This initiative will help identify and establish the means and mechanisms for the federal government to take maximum advantage of the cyber information and capabilities of the whole to produce the best overall national cyber defense possible. It will also help to better enable each agency to carry out its defined mission responsibilities.

6	Develop a Government-Wide Cyber Counterintelligence Plan	This initiative will develop a cyber counterintelligence plan to comprehensively reflect the scope and extent of cyber threats posed by adversaries who are targeting U.S. computer networks for disruption and exploitation.
7	Increase Security of the Classified Networks	This initiative will develop a detailed plan to address the security of federal government classified networks, including recommended measures that will significantly enhance the protection of these networks from the full spectrum of threats.
8	Expand Cyber Education	The intent of this initiative is to develop a strategy to build a comprehensive federal cyber education and training program, including offensive and defensive skills and capabilities. This initiative will provide a holistic education and training program that builds a workforce for the nation.
9	Define and Develop Enduring Leap-Ahead Technology, Strategies, and Programs	This initiative is intended to expand cyber research and development in high-risk, high-return areas and will evaluate new technologies to leap and stay ahead of adversaries on both defense and offense.
10	Define and Develop Enduring Deterrence Strategies and Programs	This initiative will feature a self-contained "Cyber Solarium" project in which a broad multi-disciplinary group of experts consider the range of available strategic options and development alternative constructs for warning and communication, possible roles for private and international partners, and appropriate responses for both state and non-state actors.
11	Develop Multi-Pronged Approach for Global Supply Chain Risk Management	This initiative will improve our ability to prevent and defend against commercial information technology and communications supply chain attacks on U.S government networks.
12	Define the Federal Role for Extending Cybersecurity into Critical Infrastructure	This initiative will work closely with the private sector to determine the appropriate resources and tools necessary to apply better protection for critical systems in the private sector.

	STRATEGIC ENABLER	DESCRIPTION
1	Ensure adequate support to neutralize, mitigate, and disrupt domestic illegal computer activity.	This enabler will integrate intelligence community members into the NCIJTF and enhance the FBI's Cyber and Counterintelligence resources nationwide.
2	Increase Department of Defense information assurance.	This enabler will provide the critical information assurance components to establish a defendable Department of Defense enterprise infrastructure to protect against highly sophisticated cyber adversaries and prevent attacks.
3	Increase predictive behavioral information and trend analysis.	This enabler will increase Defense Intelligence Agency analytic support to cyber operations to provide a sound, in-depth, and predictive intelligence analytic foundation.
4	[redacted]	[redacted]
5	[redacted]	[redacted]
6	Develop, deploy, and manage an automated intrusion response capability.	Description is Top Secret and has been removed from this report.
7	Monitor and coordinate the CNCI implementation.	This enabler gave the Director of National Intelligence the responsibility to coordinate and monitor the implementation of the CNCI.

APPENDIX IV

NCIJTF PARTICIPATING AGENCIES

The NCIJTF is comprised of the following member agencies:

Participating Agencies	**Executive Order 12333 Authority**
Federal Bureau of Investigation	√
[redacted]	[redacted]
National Security Agency	√
United States Secret Service	
U.S. Department of Justice	
Department of Defense Cyber Crime Center	
Naval Criminal Investigative Service	
U.S. Air Force Office of Special Investigations	√
U.S. Department of Energy	√
U.S. Department of State	√
U.S. Army 902nd Military Intelligence Group	√
U.S. Army Intelligence and Security Command	√
Joint Task Force – Global Network Operations	√
Defense Intelligence Agency	√
National Geospatial Intelligence Agency	√
U.S. Department of Homeland Security	
U.S. Army Criminal Investigative Division	
Defense Criminal Investigative Service	

APPENDIX V

CYBER DIVISION TRAINING MAP

[redacted]

APPENDIX VI

FEDERAL BUREAU OF INVESTIGATION'S RESPONSE TO THE REPORT

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

November 4, 2010

The Honorable Glenn A. Fine
Inspector General
Office of the Inspector General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Room 4322
Washington, D.C. 20530

Dear Mr. Fine:

The Federal Bureau of Investigation (FBI) appreciates the opportunity to review and respond to your draft report entitled, "The Federal Bureau of Investigation's Ability to Address the National Security Cyber Intrusion Threat" (hereinafter "Report").

We are pleased the Report found that, "[t]he FBI has completed many of the goals for the National Cyber Investigative Joint Task Force as developed under the Comprehensive National Cybersecurity Initiative and has identified techniques and tactics being used to attack United States computer networks." Indeed, the Report reflects that the FBI completed the vast majority (20 out of 22) of its Comprehensive National Cybersecurity Initiative (CNCI) milestones that were set to be accomplished by March 2010.

In addition, the accomplishments of the National Cyber Investigative Joint Task Force (NCIJTF) have also been acknowledged by the United States National Intelligence Community, Office of the Directorate of National Intelligence (ODNI) through a National Intelligence Meritorious Award issued in August 2009 to the FBI's National Security Cyber Unit and NCIJTF. Therein, the ODNI recognized the exceptional service of the alliance of peers, operators, and analysts from multiple agencies at the FBI and NCIJTF, who worked together on threats of concern from April 2007 to April 2009. As stated by ODNI, "The National Cyber Investigative Joint Task Force 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." Although not mentioned in the Report, the NCIJTF is very proud of this honorable citation.

The Honorable Glenn A. Fine

Based upon a review of the Report, the FBI concurs with the ten recommendations directed to the FBI. Enclosed herein are the FBI's responses to the recommendations. Please feel free to contact me at 202-324-0308 should you have any questions or need further information.

Sincerely yours,

T. J. Harrington
Associate Deputy Director

Enclosure

OIG Review of the FBI's Ability to Address the National Security Cyber Threat
Response to Recommendations within the Final Draft

Recommendation 1: Ensure the completion of the activities for implementing the NCIJTF as outlined in the March 2008 Office of Director of National Intelligence report on CNCI implementation.

FBI Response to Recommendation #1:
Concur. The FBI has completed all activities for implementing the NCIJTF as outlined in the March 2008 ODNI report on CNCI implementation.

Recommendation 2: Establish policies and procedures, agreed to by NCIJTF partners, for the sharing of information within the NCIJTF.

FBI Response to Recommendation #2:
Concur. The FBI will meet with the permanent NCIJTF partners [redacted] NSA, and USSS) to establish NCIJTF Information Sharing Protocols. A draft set of NCIJTF Information Sharing Protocols already has been written by Cyber Division management and is being provided to FBI OGC for review. The FBI will also seek consensus among the permanent partners for the Protocols. In the absence of consensus, the FBI will publish Interim NCIJTF Information Sharing Protocols.

Recommendation 3: Continue efforts to obtain signed Memoranda of Understanding from the NCIJTF's participating agencies.

FBI Response to Recommendation #3:
Concur. The FBI will communicate monthly with those agencies that participate in the NCIJTF but have not yet signed MOUs in order to seek their written agreement. The FBI will document the results of these communications. To the extent an agency decides it will not sign an MOU, the FBI will no longer count them as a "participating agency," and will document to those agencies the limitations on their relationship within the NCIJTF.

Recommendation 4: Enhance efforts to educate FBI field office personnel on the NCIJTF's role and use within FBI's national security cyber strategy.

FBI Response to Recommendation #4:
Concur. The FBI Cyber Division will send an electronic communication to all Field Offices which describes the NCIJTF's history, role, and use within the FBI's national security cyber strategy. The FBI Cyber Division also will post the communication on its internal website.

Recommendation 5: Ensure Cyber National Security Section program managers provide cyber agents in field offices with the operational guidance and casework coordination necessary to fully investigate national security intrusion cases effectively.

FBI Response to Recommendation #5:
Concur. The Cyber National Security Section program managers will document and distribute to all Field Offices a description of the FBIHQ resources which are available to assist Field Offices to obtain operational guidance and coordinate cases.

Recommendation 6: Evaluate the effectiveness of the step-by-step training course for FBI agents on how to investigate national security intrusion cases.

FBI Response to Recommendation #6:
Concur. The Cyber Division will initiate a Level 3 Diagnostic Audit of the Cyber Division [redacted] Training Class. This class teaches the fundamentals and case scenarios of intrusion cases, including the National Security Branch investigations within the Cyber Division. A Level 3 Diagnostic includes independent academic review of curriculum, goals, objectives, terminal objectives and testing materials.

Recommendation 7: Ensure that cyber career path agents complete the existing curriculum for all stages of the Cyber Development Plan.

FBI Response to Recommendation #7:
Concur. The FBI's Cyber Division, in collaboration with the Human Resources Division (HRD), tracks all Cyber Career Path Agent training. The Cyber Division monitors and enforces Agent completion of required and recommended training in each stage of the Cyber Developmental Plan. The Cyber Education and Development Unit (CEDU), within the Cyber Division, works continuously to ensure that all Cyber Career Path Agents complete the existing training curriculum. Cyber Division will review the current curriculum and stages of the Cyber Development Plan and consider adjustments based on cyber investigative or management responsibilities and time in position. Cyber Division will also review Cyber job posting required and preferred competencies, and provide guidance to the Field regarding the level of training that should be associated with certain positions, performance reviews, and advancement opportunities.

During fiscal year 2010 (FY10), CEDU provided each Cyber Career Path Agent with an individualized training plan. To ensure the timely completion of these training plans, CEDU created a detailed demand analysis to improve its ability to deliver the required amount of courses. Using this methodology, Cyber Career Path Agents were notified when courses were available and, based on operational needs, either accepted or declined these invitations. By offering a variety of training dates, the majority of Cyber Career Path Agents were able to attend the necessary courses based on their date of preference.

Additionally, CEDU fully implemented options to "test-out" of all required courses in the Cyber Career Path. This enabled Agents to obtain credit for courses in which they demonstrated existing competence. CEDU also increased the advertisement of the available test-out options.

Each of these efforts significantly increased Cyber Career Path Agent completion of the required curriculum. The Cyber Career Path Unit and the Cyber Education Logistics Unit (successors to CEDU) plan to continue these efforts.

Recommendation 8: Reconsider the rotation policy for cyber agents, and ensure that agents skilled and experienced in cyber intrusions are available to FBI field offices.

FBI Response to Recommendation #8:
Concur. The FBI's HRD will review the rotation policy for agents and the effects it has on various programs, to include cyber. In addition, the FBI's Transfer Unit conducts quarterly meetings with Cyber to address any experience and staffing issues.

Recommendation 9: Consider establishing a cyber intrusion specialty within the cyber career path.

FBI Response to Recommendation #9:

[redacted] **Concur.** A cyber intrusion work specialty already exists within the Cyber Career Path, which is coded and tracked in both the Bureau Personnel Management System and Virtual Academy. [redacted]

Recommendation 10: Consider developing regional hubs with agents expert in investigating national security intrusions.

FBI Response to Recommendation #10:
Concur. The FBI will complete a review of the concept of establishing regional hubs that emphasize agents expert in investigating national security intrusions.

OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT

The OIG provided a draft of this audit report to the FBI. The FBI's response is incorporated in Appendix VI of this final report. The following provides the OIG analysis of the response and summary of actions necessary to close the report.

Analysis of Actions Necessary to Resolve the Report

1. **Closed.** We recommended that the FBI ensure the completion of the activities for implementing the NCIJTF as outlined in the March 2008 Office of Director of National Intelligence report on CNCI implementation. The FBI concurred with our recommendation and, in January 2011, provided us a copy of the FBI's CNCI 4th Quarter 2010 Quarterly Report, an FBI report to the Office of the Director of National Intelligence on the FBI activities for implementing the NCIJTF.

   We reviewed this documentation and determined that it demonstrates adequate actions to address our recommendation. Therefore, this recommendation is closed.

2. **Resolved.** The FBI concurred with our recommendation to establish policies and procedures, agreed by NCIJTF partners, for the sharing of information within the NCIJTF. The FBI stated in its response that it will meet with the permanent NCIJTF partners to establish information sharing protocols. In addition, the FBI stated that it will seek consensus among the permanent partners for a draft set of NCIJTF information sharing protocols written by Cyber Division management. In the absence of consensus, the FBI stated that it will publish interim NCIJTF information sharing protocols. This recommendation can be closed when we receive documentation demonstrating that the FBI has established and NCIJTF partners have agreed to NCIJTF information sharing policies and procedures.

3. **Resolved.** The FBI concurred with our recommendation to continue efforts to obtain signed Memoranda of Understanding from NCIJTF's participating agencies. The FBI stated in its response that it will communicate monthly with those agencies that participate in the NCIJTF but have not yet signed MOUs in order to seek their written agreement.

To the extent an agency decides it will not sign an MOU, the FBI stated that it will no longer count the agency as a "participating agency" and will document to such agency the limitations on its relationship within the NCIJTF. This recommendation can be closed when we receive signed MOUs from each participating agency.

4. **Resolved.** The FBI concurred with our recommendation to enhance efforts to educate FBI field office personnel on the NCIJTF's role and use within FBI's national security cyber strategy. The FBI stated in its response that the FBI Cyber Division will send to all field offices and post on its internal website an electronic communication describing the NCIJTF's history, role, and use within the FBI's national security cyber strategy. This recommendation can be closed when we receive this Cyber Division electronic communication and evidence that the information is posted on the FBI's internal website.

5. **Resolved.** The FBI concurred with our recommendation to ensure Cyber National Security Section program managers provide cyber agents in field offices with the operational guidance and casework coordination necessary to fully investigate national security intrusion cases effectively. The FBI stated in its response that the Cyber National Security Section program managers will document and distribute to all field offices a description of the FBIHQ resources which are available to assist field offices to obtain operational guidance and coordinate cases. This recommendation can be closed when we receive documentation demonstrating that the program managers provided this guidance to help field offices necessary fully investigate national security intrusion cases effectively.

6. **Resolved.** The FBI concurred with our recommendation to evaluate the effectiveness of the step-by-step training course for FBI agents on how to investigate national security intrusion cases. The FBI stated in its response that the Cyber Division will initiate a Level 3 Diagnostic Audit of the Cyber Division [redacted] Training Class, which the FBI noted is intended to teach the fundamentals and case scenarios of cyber intrusion cases. This recommendation can be closed when we received the results of the FBI's Level 3 Diagnostic Audit of this training class along with an FBI action plan making necessary improvements to the course.

7. **Resolved.** The FBI concurred with our recommendation to ensure the cyber career path agents complete the existing curriculum for all stages of the Cyber Development Plan. The FBI stated in its response that the FBI's Cyber Division, in collaboration with the Human Resources

Division, tracks all Cyber Career Path Agent training. The FBI stated that the Cyber Division will review the current curriculum and stages of the Cyber Development Plan and consider adjustments based on cyber investigative or management responsibilities and time in position. The FBI also stated that the Cyber Division will review Cyber job posting required and preferred competencies, and provide guidance to the field regarding the level of training that should be associated with certain positions, performance reviews, and advancement opportunities. This recommendation can be closed when we received documentation demonstrating that cyber agents are completing the existing curriculum for all stages of the Cyber Development Plan based on the time in position.

8. **Resolved.** The FBI concurred with our recommendation to reconsider the rotation policy for cyber agents, and ensure that agents skilled and experienced in cyber intrusions are available to FBI field offices. The FBI stated in its response that FBI's Human Resources Division will review the effects the FBI's rotation policy for agents has on various programs, including its cyber program. This recommendation can be closed when we receive documentation demonstrating the results of the FBI's Human Resources Division review of the FBI's rotation policy, and evidence of any actions taken to ensure agents skilled and experienced in cyber intrusion investigations are available to FBI field offices.

9. **Resolved.** The FBI concurred with our recommendation to consider establishing a cyber intrusion specialty within the cyber career path. The FBI stated in its response that a cyber intrusion work specialty already exists within the Cyber Career Path, which is coded and tracked in the Bureau Personnel Management System and Virtual Academy. This recommendation can be closed when we receive documentation demonstrating that the FBI has considered establishing a cyber intrusion specialty within the cyber career path with prescribed knowledge, skills, abilities, responsibilities, and training for agents assigned to this specialty area.

10. **Resolved.** The FBI concurred with our recommendation to consider developing regional hubs with agent experts in investigating national security intrusions. The FBI stated in its response that it will complete a review of the concept of establishing regional hubs that emphasize agent expert in investigating national security intrusions. This recommendation can be closed when we receive the results of the FBI's review of, as well as any plan for, establishing regional hubs for national security intrusion investigations.