



**U.S. Department of Justice
Office of the Inspector General
Evaluation and Inspection Division**

**Federal Bureau of Investigation's
Integrity and Compliance Program**

November 2011

I-2012-001

EXECUTIVE DIGEST

In June 2007, the Federal Bureau of Investigation (FBI) established the Integrity and Compliance Program (ICP) to identify and mitigate legal compliance risks within the FBI.¹ The ICP is designed to proactively identify and correct weaknesses in policy, training, monitoring, and auditing that could result in FBI employees violating the law as they conduct their work. The ICP is modeled on corporate compliance programs that institute systematic procedures to ensure that companies adhere to the laws that govern them.

The ICP's goal is to prevent FBI employees from violating the laws and policies that govern their work by: (1) managing the Ethics and Standards of Conduct program (ethics program) and (2) identifying and reducing legal compliance risks in operations FBI-wide and at the program level.² The FBI's Office of Integrity and Compliance (OIC) manages the ICP.³ The OIC's mission is to "develop, implement and oversee a program that ensures that there are processes and procedures in place that facilitate FBI compliance with both the letter and spirit of all applicable laws, regulations, and policies."⁴ The purpose of this Office of the Inspector General (OIG) review was to evaluate the effectiveness of the ICP.

According to an FBI report about the ICP, the impetus for the FBI's establishment of the ICP was a 2007 OIG report that found FBI personnel had not complied with laws and policies governing the use of National Security Letter authority.⁵ The OIG report stated that the FBI issued these letters

¹ The FBI defines a legal compliance risk as potential harm to the FBI caused by failures of FBI personnel to comply with the laws and policies governing FBI operations.

² The FBI plans to expand its bureau-wide and program-level efforts to identify and reduce legal compliance risks in the future to include the participation of field office personnel.

³ The ICP is not a separate office within the FBI. Except for OIC staff members who manage the program full time, the remaining work of the program is conducted by FBI employees and committees who do the work of the program in addition to their regular duties. In this report we attribute actions to the ICP to convey that various individuals or entities are collectively performing the ICP's functions.

⁴ FBI Policy Directive 0002D, FBI Integrity and Compliance Program, June 25, 2007.

⁵ FBI, *The 2008 State of the Integrity and Compliance Program*, and U.S. Department of Justice Office of the Inspector General, *Review of the Federal Bureau of Investigation's Use of National Security Letters* (March 9, 2007). Under five statutory provisions, the FBI can use National Security Letters to obtain – without a court order – records such as customer

(Cont'd.)

without proper authorization, made requests outside of the scope allowed by statute, and conducted unauthorized collection of telephone or Internet e-mail transactional records.

At the FBI-wide level, FBI executives identify, analyze, and mitigate legal compliance risks that affect the FBI as a whole and that may involve coordination between more than one functional area within, and sometimes outside of, the FBI to resolve. At the FBI-wide level, FBI executives identify and direct actions through a series of steps: risk identification, risk prioritization and selection, risk analysis, risk mitigation, and audit. OIC staff members manage each step of this process, and different FBI committees and employees provide the subject matter expertise needed at each step. In addition, the FBI Inspection Division audits the steps taken to mitigate the risks to determine whether the identified risks actually have been reduced.

At the program level, managers of the FBI's 53 major programs identify and mitigate risks that do not involve coordination outside of their program areas to resolve. These managers are responsible for programs that encompass the FBI's operations and administrative functions, ranging from counterintelligence to violent crime and from information technology management to fleet management and transportation services.⁶ Managers of the major programs identify their highest priority compliance risks and submit reports twice a year to the OIC and to their divisions' Assistant Directors that include descriptions of the identified risks and the program managers' plans for mitigating them. The OIC reviews these reports to make sure that the issues identified are legal risks and that the plans to address the risks are realistic and can be reasonably expected to reduce the risks. According to the template program managers use in developing risk mitigation plans, their process should also include an audit or a way to monitor the mitigation steps.

Additionally, the OIC manages the FBI's ethics program, which entails providing guidance and training to employees that emphasize the importance of complying with laws and policies that govern their work and the importance of reporting non-compliance with those laws and policies. The OIC is also

information from telephone companies, Internet service providers, financial institutions, and consumer credit companies.

⁶ While there are many programs in the FBI, this review focused on the FBI's 53 major programs because these are the only programs the ICP requires to report to the OIC. The OIC determined the FBI's 53 major programs by reviewing budget data, consulting with the FBI's Inspection Division to identify programs that are required to periodically report on their performance to that division, and after review and approval by senior management.

responsible for maintaining open communication channels for FBI employees to report compliance concerns and for assessing the ICP.

RESULTS IN BRIEF

Through the ICP, the FBI implemented strategies that have started to reduce legal compliance risk in FBI operations. We found that, since the ICP's inception in 2007, the ICP has used a variety of sources to identify 206 FBI-wide potential risk indicators and 112 program-level risks.⁷ As will be explained below, these risks have included potential non-compliance in the FBI's use of administrative subpoenas and confidential human sources, as well as potential criticism and litigation over backlogs of DNA samples. In addition, the FBI has taken steps to reduce risk by implementing mitigation plans for 13 FBI-wide risks and 16 program-level risks.⁸ We reviewed 11 of the 13 FBI-wide plans and determined that the process the ICP used to develop them addressed the areas of compliance risk and involved relevant stakeholders. Based on the thoroughness of these plans, we believe that if the FBI implements the actions as described, it is reasonable to expect that the actions will reduce compliance risk in those areas. In addition, there were five risk areas where we assessed evidence about whether compliance risk was reduced and found that it was reduced in three of these areas. Further, the OIC manages and has enhanced the FBI's ethics program and promotes reporting of compliance concerns.

However, we identified areas for improvement in the ICP that, if addressed, could enhance its effectiveness and sustainability. We found that most FBI executives and managers no longer consistently use the risk assessment methodology designed for the ICP to evaluate identified risks. Currently, risk assessment and selection is informal, unsystematic, and undocumented, resulting in ICP participants not necessarily considering the factors identified by the FBI to prioritize risk, which can result in a prioritization inconsistent with the program's established goals.

Further, at the program level, there is no verification that mitigation actions are complete and effective in reducing compliance risk. Because of this lack of monitoring, the FBI cannot be sure that it has successfully implemented the risk reduction strategies for the selected risks. Also, the ICP has not yet been fully implemented in field divisions and, as a result, the field

⁷ Before Executive Management Committees review potential risks and determine whether they may be a concern for the FBI, the FBI considers them "potential risk indicators."

⁸ According to the FBI, since the ICP's inception, at the FBI-wide level, 26 risk mitigation plans have been developed and approved to address identified risks but only 13 have been implemented.

divisions' role in risk identification and reporting to the OIC is undeveloped. Finally, the OIC has not established a way to evaluate the ICP's overall effectiveness or the effectiveness of its processes. Without evaluation, the OIC cannot identify where changes in the program should occur or ensure the sustainability of the ICP.

The following sections discuss our findings in more detail.

Through the ICP, the FBI implemented strategies that have started to reduce compliance risk in FBI operations and activities.

The ICP's identification and mitigation of legal compliance risks before they develop into problems have the potential to significantly reduce legal compliance risk in the FBI operations. Prior to the ICP, the FBI identified and addressed compliance risks unsystematically through efforts that were generally stove-piped within specific divisions. Now the FBI addresses compliance risks systematically and in a way that involves relevant stakeholders and subject matter experts within and outside of the FBI. The following two sections discuss the ICP's efforts to reduce legal compliance risk in more detail.

The ICP has identified risks using a variety of sources.

We found that the ICP uses a variety of sources at both the FBI-wide and the program levels to identify compliance risks, as FBI policy requires.⁹ Sources include FBI executives, program managers, employees, and open source information such as newspaper articles and government oversight reports. The ICP's establishment of a systematic process for risk identification has improved the FBI's ability to identify potential compliance risks and senior management's knowledge of compliance weaknesses. According to the FBI Director, one of the most important aspects of the ICP is that it identifies gaps and vulnerabilities.

At the FBI-wide level, there are five Executive Management Committees that identify and select risks to mitigate. Each committee identifies and selects risks that pertain to its functional branch. The five Executive Management Committees corresponding with the FBI's branches are administrative; criminal, cyber, response, and services; information technology; national security; and science and technology.¹⁰ Each committee is chaired by the

⁹ FBI Policy Directive 0002D, FBI Integrity and Compliance Program, June 25, 2007.

¹⁰ The administrative Executive Management Committee is made up of the Human Resources Branch and various entities in the FBI Director's Office with administrative responsibilities.

Executive Assistant Director in charge of that branch and includes the Assistant Directors in charge of the divisions within that branch. The committees meet quarterly to discuss the progress toward mitigating previously identified risks that were selected for mitigation and to identify new risks to address.

FBI executives told us that they identified risks based on knowledge of their branches and through consultation with the managers within their branches and divisions. In addition, the OIC provides FBI executives with Leading Risk Indicator Reports that summarize the risks the OIC staff compile from its own research of open source information, government reports, and new regulations, and from risks that individual FBI employees and employee groups report to the OIC. From the ICP's inception in 2007 to August 2011, the FBI identified 206 indicators of potential FBI-wide risk to be considered by the 5 Executive Committees and selected 50 of those risks for analysis and potential mitigation.

At the program level, the managers in charge of the 53 major programs are required to determine their highest priority risk within their programs and report their selections to the OIC in bi-annual reports. The programs that are required to participate span 20 different FBI divisions and all 5 of the FBI's functional branches. In a sample of bi-annual reports covering actions initiated before or during the reporting period of December 2009 to June 2010, we found that 44 program areas reported program risks. Of the nine other programs, the OIC had exempted three from reporting program risks. The remaining six program area managers had not submitted reports. In these instances, the OIC directed managers to identify and submit risks "in accordance with FBI policy" in their next bi-annual reports.

Through the ICP, the FBI took steps to reduce legal compliance risk by implementing mitigation plans.

The ICP has implemented mitigation plans at both the FBI-wide and program levels. At the FBI-wide level, the ICP implemented 13 mitigation plans. We reviewed 11 of these plans.¹¹ Five of the implemented plans had been audited. We found that the mitigation steps the FBI implemented for three of the five audited plans sufficiently mitigated the risks, but additional efforts were required to completely mitigate the other two plans.¹² Although

¹¹ We did not review 2 of the 13 implemented mitigation plans because they contained classified material, and we determined that access to that material was not essential to our review.

¹² We could not conclude that the FBI reduced actual non-compliance because it did not establish baselines of non-compliance before implementing mitigation steps that we could
(Cont'd.)

the mitigation plans for the remaining six risks appear reasonable, we cannot determine whether they have mitigated the risks because information necessary for us to make this assessment (such as an audit or mitigation action that we could observe in the field) was not available at the time of our review. We provide examples of these risks, the actions the ICP took to mitigate them, and the outcomes of the mitigation steps in the body of this report.

At the program level, we reviewed the reports that program managers submitted to the OIC covering their risk mitigation work completed or initiated between December 2009 and July 2010. We found that OIC staff members had determined 16 risks to be closed (mitigated) and that managers had begun to mitigate an additional 86 risks. We cannot conclude that compliance risk in these areas was mitigated because the ICP does not require verification of program-level mitigation actions, but the mitigation actions for 5 of the 16 risks established internal controls that we believe could reasonably be expected to reduce the risk.

The remaining 11 risks entailed mitigation actions, such as issuing additional guidance, but did not specify the establishment of internal controls, or additional internal controls if regular monitoring efforts were already in place, which would have provided more assurance of the mitigations' effectiveness. While the actions established in the mitigations appear reasonable, without adequate verification that they resulted in the needed changes, it is not possible to know whether the steps were adequate or whether additional steps are required. For example the National Name Check Program, which disseminates information from FBI files to other federal agencies when requested, identified a risk that inadvertent release of protected information might occur. To mitigate the risk, the program developed a standard operating procedure to prevent inadvertent release of protected information. It also required all National Name Check Program employees to attend annual training covering the guidelines for disseminating certain information. However, other than the Quality Assurance Program that was already in place, which reviews about 10 percent of outgoing work, no monitoring was put into place to see if the training was successful or if the risk of inadvertent disclosure was mitigated.

In some cases, such as in the example above, there may be a monitoring mechanism in place, but in current practice program managers do not always share information about the existing monitoring or its results with the OIC. If the OIC is not aware of monitoring and the program does not report the results

compare to non-compliance after implementation. The ICP does not measure whether its actions reduce non-compliance.

of monitoring efforts, there is still no way to ensure that the risk mitigation occurred and was effective.

The OIC manages the FBI's ethics program and promotes reporting of compliance concerns.

The OIC established and maintains open communication channels for FBI employees, and the FBI supported the OIC's objectives by establishing new human resource initiatives that encourage compliance and reporting of compliance concerns. For example, the OIC developed new ethics training videos and issued a non-retaliation policy for reporting compliance concerns. We also examined all complaints of retaliation by FBI employees between January 2007 and February 2011 and found no case in which an employee who reported a compliance concern to the OIC later reported being retaliated against for doing so.

However, during our site visits we found that most field division employees we interviewed were unaware of two of the new human resource initiatives that affect them: the Compliance Helpline employees can call anonymously to report compliance concerns and an award to recognize employees for supporting the ICP. We found that only 20 percent (14 of 70) of the field division employees were aware of the Compliance Helpline and only 13 percent (8 of 64) were aware of the award. This lack of awareness limits the effectiveness of these OIC efforts to promote the reporting of compliance concerns throughout the FBI.

The FBI could improve the ICP's effectiveness and sustainability by addressing certain factors.

We identified areas for improvement in the ICP at both the FBI-wide and program levels. We found that FBI executives and managers do not use the risk assessment methodology the ICP designed to evaluate risks. Instead, risk assessment and selection are informal, unsystematic, and undocumented. In addition, the ICP does not have a method to ensure that mitigation actions effectively address program-level risks. Further, the ICP is not fully implemented in field divisions. Finally, the ICP has not established a way to measure progress toward achievement of its goals. Each of these areas for improvement is discussed in the sections below.

FBI executives and managers are not using the ICP's risk assessment methodology, causing risk selection to be informal, unsystematic, and undocumented.

The FBI developed a risk assessment methodology based on its research of best practices of corporate compliance programs (see text box) and the factors of risk it deemed important. The OIG used the methodology initially to help FBI executives understand how to assess risk in the ICP, and executives used the methodology to rank risks that they identified early on in the ICP. However, at the FBI-wide level, only one of the five committees of executives currently uses the methodology at all, and that committee's use of it is limited. In lieu of using the risk assessment methodology, FBI executives' process for prioritizing and selecting risks for mitigation has been informal and based on discussion that was not documented. FBI executives we interviewed told us that they assessed risk through discussion before and during the quarterly Executive Management Committee meetings. The minutes of these meetings include updates on the mitigation actions for risks selected for mitigation, but do not document how participants prioritized or selected risks.

The FBI's Risk Assessment Methodology

To prioritize risks, the FBI developed a methodology to determine a numeric score for each risk based on the frequency of the activity, consequence of non-compliance, and the probability of non-compliance. The first six factors below help determine the probability of non-compliance. The seventh factor helps to determine the consequence of the activity. Participants also were to consider potential for legal action and reputational harm to the FBI when assessing consequence.

1. *Complexity.* Does activity occur in multiple locations or internationally, involve external agencies, or have many legal requirements?
2. *Internal Risk Indicators.* Is there a history of compliance issues? Is there an existing process to assess risk in the area?
3. *External Risk Indicators.* Have other agencies had problems with the activity? Is there a trend in civil liability or overturned convictions, or external reports citing compliance issues?
4. *Environment.* Is the activity new or does it require new technology? Is there pressure to conduct the activity?
5. *Workforce.* Is there turnover among key personnel? Is the workforce experienced and adequately trained?
6. *Internal Work Process.* Is activity manual or automated? Does it allow individual discretion? Does it require approval and monitoring? Are responsibilities clearly defined?
7. *Impact on Privacy and Civil Liberties.* Does activity affect privacy, First Amendment rights, individuals directly, or other civil liberties?

Similarly, at the program level, only 29 percent (13 out of 45) of the managers who responded to a survey we conducted reported using the methodology or the factors in it to determine their program's risks. The remaining 71 percent (32 out of 45) appeared to be using their own criteria.

We found risk prioritization and selection at the program level is also informal and undocumented. Program managers describe the risks they have identified and their plan to mitigate them in written reports to the OIC. The process does not require in-person contact between OIC staff members and managers.

Requiring a consistent methodology for assessing risk would help the ICP communicate its expectations about the factors to consider in prioritizing and selecting risks to new participants and participants who may not receive in-person guidance in identifying risks. Because the FBI plans to expand field division participation in the ICP and because the FBI's rotation policy ensures that the ICP will constantly have new participants, using established factors is important for the ICP's effectiveness.

Using this risk assessment methodology would also ensure that participants consider the risk factors the FBI deems important. For example, one of the factors included in the methodology the OIC designed for the ICP is a risk's impact on privacy and civil liberties. This is an important factor, but at the FBI-wide level only 33 percent (5 of 15) of executives we interviewed said that they considered this factor when they made their assessments.¹³ If FBI executives and program managers are not using the methodology, they may not consider this factor when comparing risks, even though threats to privacy and civil liberties caused by the FBI's misuse of its National Security Letter authority was a significant reason the FBI established the ICP.¹⁴

The ICP does not require external verification for major program mitigation efforts, and the OIC lacks the authority to require program-level participation.

At the program level, we found that the ICP lacks a way to ensure that risk reduction strategies are implemented and that they reduce compliance risks. Program-level mitigation does not include any independent assessment of implemented strategies. In no case did we find that a mitigated program risk had external verification to ensure that the mitigation actions had been taken and to assess the effectiveness of those actions. Verification could be as simple as someone checking that the plan is implemented and operational, and that the risk appears to be mitigated. Without this step, the ICP cannot ensure that managers' mitigation actions are complete or effective.

¹³ The other 10 executives may also have considered this factor but they did not tell us that they did when we asked, "What factors do you consider when assessing risks?"

¹⁴ U.S. Department of Justice Office of the Inspector General, *Review of the Federal Bureau of Investigation's Use of National Security Letters* (March 9, 2007).

Additionally, the OIC staff oversees the program-level risk mitigation, but does not have the authority to require program managers to participate. FBI policy requires major program managers to participate in the ICP, but we found that 6 of 53 (11 percent) major program managers did not.¹⁵ In these instances, the OIC directed managers to identify and submit risks “in accordance with FBI policy” in their next bi-annual reports.¹⁶ Assistant Directors directly supervise program managers and could ensure managers’ participation, but we found that only one of the nine Assistant Directors we asked about program-level risk mitigation was aware of it. Four of the 10 OIC staff members we asked said that Assistant Director buy-in to program-level mitigation was important but not consistent. Involving Assistant Directors would help ensure that program managers prioritize program-level risk mitigation.

The ICP is not fully implemented in field divisions.

While there are plans to implement risk identification and mitigation in field divisions in the future, the OIC Assistant Director stated that the focus of the ICP has been to implement the program first at headquarters. Nonetheless, in 2007, the FBI created the Division Compliance Officer position as a collateral duty in FBI field divisions to provide a single point of contact for each field division to support the ICP.¹⁷ We found that, as of fall 2010, field divisions had appointed Division Compliance Officers, but the OIC had not fully developed or used this position. The OIC also had not established a method to identify and mitigate compliance risks in field divisions. The three Division Compliance Officers in the field divisions we visited indicated that they did not yet perform any additional tasks as the point of contact for the OIC.

In August 2011, the OIC’s Assistant Director gave us a draft policy that, if approved, would formally implement the ICP in the field. This policy would clarify the role of the Division Compliance Officer and require all field divisions to implement division compliance councils. These councils would identify potential compliance risks to determine whether they constitute actual risk within a division. Once actual risks are identified, the councils would develop, implement, and track mitigation plans to completion. The councils would

¹⁵ FBI Policy Directive 0126D, Application of the Integrity and Compliance Program to FBI Program Management, October 24, 2008.

¹⁶ In the bi-annual reports, which are reviewed by OIC staff, program managers are to include a description of risks identified and their plan for mitigating the highest priority risk.

¹⁷ FBI Policy Directive 0005D, FBI Division Compliance Officer, October 1, 2007.

inform the OIC of compliance risks that could affect multiple field divisions or the FBI as a whole.

The OIC has not established a way to assess the ICP's overall effectiveness or to measure progress toward achievement of ICP goals.

The OIC has not evaluated the effectiveness of the ICP since 2008 or measured its progress toward achievement of the ICP's goals. FBI policy states that "the OIC shall evaluate the effectiveness of and prepare and deliver to FBI senior management an annual report on the state of the ICP."¹⁸ However, since the initial report in 2008, the OIC has not prepared this report. Currently the ICP uses a regular survey to assess FBI employees' attitudes toward compliance every 18 months and a monthly report to track progress toward mitigating specific risks. However, the OIC lacks a method or report for providing an assessment of the ICP overall. Without a way to assess the ICP and a way to measure progress toward accomplishment of the ICP's goals, the OIC cannot determine the ICP's effectiveness at reducing compliance risk or identify where changes in the program should occur to ensure the sustainability of the ICP.

CONCLUSION AND RECOMMENDATIONS

We conclude that while there remain areas for improvement in the FBI's ICP, the program is implementing risk reduction strategies throughout the FBI and has begun to reduce compliance risk. The ICP's identification, analysis, and mitigation of legal compliance risks FBI-wide and at the program level before they develop into problems has the potential to significantly reduce legal compliance risk in FBI operations. We found that three of the five implemented mitigation plans at the FBI-wide level reduced compliance risk by making changes to areas such as policy, training, and operations. We believe that the concept of the FBI's OIC program has been beneficial to its efforts to monitor and enhance compliance with legal requirements, and that other agencies may wish to consider implementing a similar kind of program.

We also identified several areas in the ICP that, if refined, could improve the FBI's ability to reduce legal compliance risk and the ICP's sustainability. First, increasing employee awareness of the Compliance Helpline and other OIC human resource initiatives could further promote a culture of compliance and the reporting of compliance concerns.

Second, FBI executives and managers are not using the ICP's risk assessment methodology, causing risk selection to be informal, unsystematic,

¹⁸ FBI Policy Directive 0002D, FBI Integrity and Compliance Program, June 25, 2007.

and undocumented. Consequently, current and future participants in the processes, particularly those at the field division level, may not know how they are to select risks and may not consider all the factors the FBI deems important. Third, the FBI cannot ensure that program-level risks are fully mitigated because the ICP does not require verification of program-level risk mitigation actions and Assistant Director involvement in program mitigation is lacking.

Fourth, the ICP is not fully implemented in field divisions. Each field division appointed a Division Compliance Officer, but the OIC has not fully developed or used this position or established a method to identify and mitigate compliance risks in field divisions. Because field division employees are more likely to report compliance concerns to officials within their field division rather than to headquarters, the ICP's effectiveness at identifying compliance risks affecting the field depends on the Division Compliance Officer's role being developed through a structure for risk identification and mitigation.

Finally, the OIC has not yet established a way to measure progress toward accomplishment of the ICP's goals and does not prepare annual reports of the ICP's activities as required. As a result, the OIC does not have a way to assess the ICP's effectiveness or to identify where changes in the program should occur.

In this report, we make five recommendations to the FBI to help the ICP improve its efforts to reduce legal compliance risks. For example, we recommend that the OIC increase awareness of the Compliance Helpline and other OIC human resource initiatives. In addition, we recommend that the FBI consider using a formal risk assessment methodology that includes a specific list of criteria that must be considered. To enhance the effectiveness of mitigation at the program level, we recommend increased Assistant Director involvement and that the ICP require program-level risk mitigation to include a verification step. To ensure that the FBI can assess the overall effectiveness of the ICP, we recommend that it comply with existing requirements for an annual report assessing the effectiveness of the ICP; for example, a report that articulates the program's goals, shows progress toward accomplishing them, and identifies areas for improvement.

TABLE OF CONTENTS

BACKGROUND 1

RESULTS OF THE REVIEW 13

 The ICP is beginning to reduce the FBI’s compliance risk 13

 Addressing areas for improvement could enhance the
 ICP’s Effectiveness 26

CONCLUSION AND RECOMMENDATIONS 35

APPENDIX I: FBI COMPLIANCE PROGRAM POLICIES 37

APPENDIX II: LIST OF FBI MAJOR PROGRAMS 38

APPENDIX III: METHODOLOGY OF THE OIG REVIEW 40

APPENDIX IV: FBI STRATEGIC SHIFTS ANTICIPATED BY OIC 44

APPENDIX V: FBI EMPLOYEE SURVEY QUESTIONS 45

APPENDIX VI: FBI RESPONSE TO DRAFT REPORT 46

APPENDIX VII: OIG ANALYSIS OF FBI RESPONSE 49

BACKGROUND

In June 2007, the Federal Bureau of Investigation (FBI) established the Integrity and Compliance Program (ICP) to proactively identify and correct weaknesses in policy, training, monitoring, and auditing that could result in FBI employees violating the law as they conduct their work. The FBI defines a legal compliance risk as harm to the FBI caused by failures of FBI personnel to comply with the laws and policies governing FBI operations. The ICP is modeled on corporate compliance programs that institute systematic procedures to ensure that companies adhere to the laws that govern them.

According to the FBI's *2008 State of the Integrity and Compliance Program* report, the impetus for the FBI's establishment of the ICP was a 2007 Office of the Inspector General (OIG) report that found FBI personnel had not complied with laws and policies governing the use of National Security Letter authority.¹⁹ The OIG report stated that the FBI had issued these letters without proper authorization, made requests outside of the scope allowed by statute, and conducted unauthorized collection of telephone or Internet e-mail transactional records.

We conducted this review to assess the performance of the FBI's ICP. The objectives of this review were to evaluate how the FBI's ICP: (1) identifies risks of non-compliance with laws, regulations, rules, and FBI and Department of Justice policies; (2) assesses identified risks; (3) analyzes highly ranked risks; (4) mitigates risks with adequate corrective actions; (5) monitors the implementation of the corrective actions to ensure that mitigation is effective; and (6) promotes a culture of integrity and ethical compliance throughout the FBI.

The Integrity and Compliance Program

The ICP's goal is to prevent FBI employees from violating the laws and policies that govern their work: (1) through operation of the FBI's Ethics and Standards of Conduct program, which entails providing guidance and training that emphasize the importance of complying with laws and policies, and of reporting non-compliance; and (2) by identifying and reducing legal compliance

¹⁹ U.S. Department of Justice Office of the Inspector General, *Review of the Federal Bureau of Investigation's Use of National Security Letters* (March 9, 2007). Under five statutory provisions, the FBI can use National Security Letters to obtain – without a court order – records such as customer information from telephone companies, Internet service providers, financial institutions, and consumer credit companies.

risks in FBI operations FBI-wide and at the program level. There are also plans to expand the ICP's risk identification and mitigation efforts to FBI field divisions in the future.

The ICP is a multi-level program and involves staff at various levels of the FBI. At the FBI-wide level, FBI executives identify, analyze, and mitigate legal compliance risks that affect the FBI as a whole and that may involve coordination between more than one functional area within the FBI, and sometimes outside of, the FBI to resolve. At the program level, FBI program managers identify, analyze, and mitigate risks within their programs that can be resolved through changes internal to those programs. FBI employees participate in the ICP through several committees and groups, and through direct interaction with the FBI's Office of Integrity and Compliance (OIC), which manages the ICP. The FBI's Inspection Division and the FBI's Office of General Counsel also have ongoing roles in risk identification and mitigation, and other FBI employees take part in the ICP as needed.

In the sections below we describe in more detail the OIC's role in managing the ICP and in risk identification and mitigation at the FBI-wide level, program level, and in FBI field divisions.

Office of Integrity and Compliance

The OIC is an independent office within the Office of the FBI Director. Its mission is to "develop, implement and oversee a program that ensures that there are processes and procedures in place that facilitate FBI compliance with both the letter and spirit of all applicable laws, regulations, and policies."²⁰ The OIC does this by managing the ICP's risk identification, analysis, and mitigation efforts at the FBI-wide and program levels (which we discuss later in this Background section), managing the FBI's Ethics and Standards of Conduct Program, and by maintaining channels of communication for reporting compliance concerns. The OIC is also responsible for assessing the ICP. The OIC is led by an Assistant Director and consists of one Unit Chief, nine Attorneys, two Management Program Analysts, one Supervisory Special Agent, and one administrative staff member. The OIC's staff members are the only FBI employees who work exclusively on the ICP.

²⁰ FBI Policy Directive 0002D, FBI Integrity and Compliance Program, June 25, 2007.

The OIC is responsible for managing the FBI's Ethics and Standards of Conduct Program.

In 2007, the FBI's Ethics and Standards of Conduct Program became a part of the ICP and is managed by the OIC. The purpose of the Ethics and Standards of Conduct Program is to "promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law."²¹ The FBI refers to this as "a culture of compliance." The program includes ensuring that the FBI complies with financial disclosure reporting requirements; conducting training for new employees on FBI and government ethics policies and providing in-service ethics training and information to existing employees; maintaining up-to-date policies and guidance on ethics requirements; and responding to employees' specific questions about whether certain activities are allowable. For example, employees may need help knowing when and if they are allowed to accept gifts or whether they need to report certain activities. In addition to these activities, the OIC assesses the FBI's "culture of compliance" using questions it added to the FBI employee survey. The FBI conducts this survey of its employees every 18 months to assess the employees' perspectives on topics related to their work environment.

The OIC is responsible for maintaining "open and effective" communication for reporting compliance concerns.

To fulfill its responsibility to maintain open and effective communication, the OIC developed FBI policy directives and human resource initiatives that outline the roles and responsibilities of FBI divisions, ICP committees, and employees (see Appendix I). For example, the ICP requires that all FBI employees report any known or suspected violations of law or FBI policy that they observe.²²

In September 2008, the OIC established a Compliance Helpline for FBI employees to call to report compliance concerns anonymously. The helpline is operated by a contractor that receives the calls and relays the reported concerns to the OIC. Employees can also report concerns directly to OIC staff using any method, including telephone, e-mail, mail, or in person. The OIC assesses each concern, forwards it to the FBI division to which it pertains, and – unless the concern was reported anonymously – contacts the employee

²¹ Office of Integrity and Compliance, FBI Integrity and Compliance Program: An Overview, slide presentation, May 19, 2010.

²² FBI Policy Directive 0003D, FBI Integrity and Compliance Executive Management Committees Charter, June 25, 2007.

who reported the concern to tell them how the FBI division to which it was assigned will address it.

Additionally, the OIC established human resource initiatives to encourage the reporting of compliance concerns. These initiatives included the addition of compliance elements to employee performance appraisals, the establishment of awards that reward employees who support the ICP, and the creation of a non-retaliation policy that states that “employees must be comfortable raising compliance concerns without fear of retaliation.”²³

The OIC is responsible for assessing the ICP.

FBI policy also assigns responsibility for assessing the ICP’s performance to the OIC. Specifically, policy requires the OIC to evaluate the effectiveness of the ICP through an annual report and to support the ICP in evaluating risk-mitigation measures.

FBI-wide Risk Identification and Mitigation

In July 2007, the ICP established a method through which FBI executives identify and address FBI-wide compliance risks through a series of steps: identification, prioritization and selection, analysis, mitigation, and audit. OIC staff members manage each step, and different FBI committees and employees provide the subject matter expertise needed at each step. The following sections present the roles and responsibilities as well as the steps taken to identify and mitigate FBI-wide legal compliance risks.

The Integrity and Compliance Council oversees the ICP and five committees of FBI executives identify and mitigate FBI-wide risks.

Integrity and Compliance Council. The Integrity and Compliance Council oversees the ICP and meets three times a year.²⁴ It is chaired by the FBI Director, and its members are the Deputy Director, the Associate Deputy Director, the five Executive Assistant Directors, the Chief Financial Officer, the General Counsel, and the Assistant Director of the OIC, who attends meetings and provides reports on the activities of the ICP. As Council Chairperson, the Director designates the top 10 compliance risks confronting the FBI. The Director may also identify risks for analysis.

²³ FBI Policy Directive 0032D, Non-retaliation for Reporting Compliance Risks, February 11, 2008.

²⁴ FBI Policy Directive 0004D, FBI Integrity and Compliance Council Charter, June 25, 2007.

Executive Management Committees. Executive Management Committees meet quarterly to identify risks for the FBI to address, select which risks to analyze and mitigate, and discuss the status of mitigation plans previously initiated.²⁵ There are five Executive Management Committees, one for each of the FBI's five branches or functional areas (see Table 1). An Executive Assistant Director chairs each Executive Management Committee. Committee membership includes the Assistant Directors of each division within that branch, the Assistant Director of the OIC, and representation from the Office of the General Counsel. At least one OIC staff member also attends. FBI policy also states that representatives from small, medium, and large FBI field divisions participate in the Executive Management Committees.

²⁵ FBI Policy Directive 0003D, FBI Integrity and Compliance Executive Management Committees Charter, June 25, 2007.

Table 1: Executive Management Committees and Their Corresponding Divisions

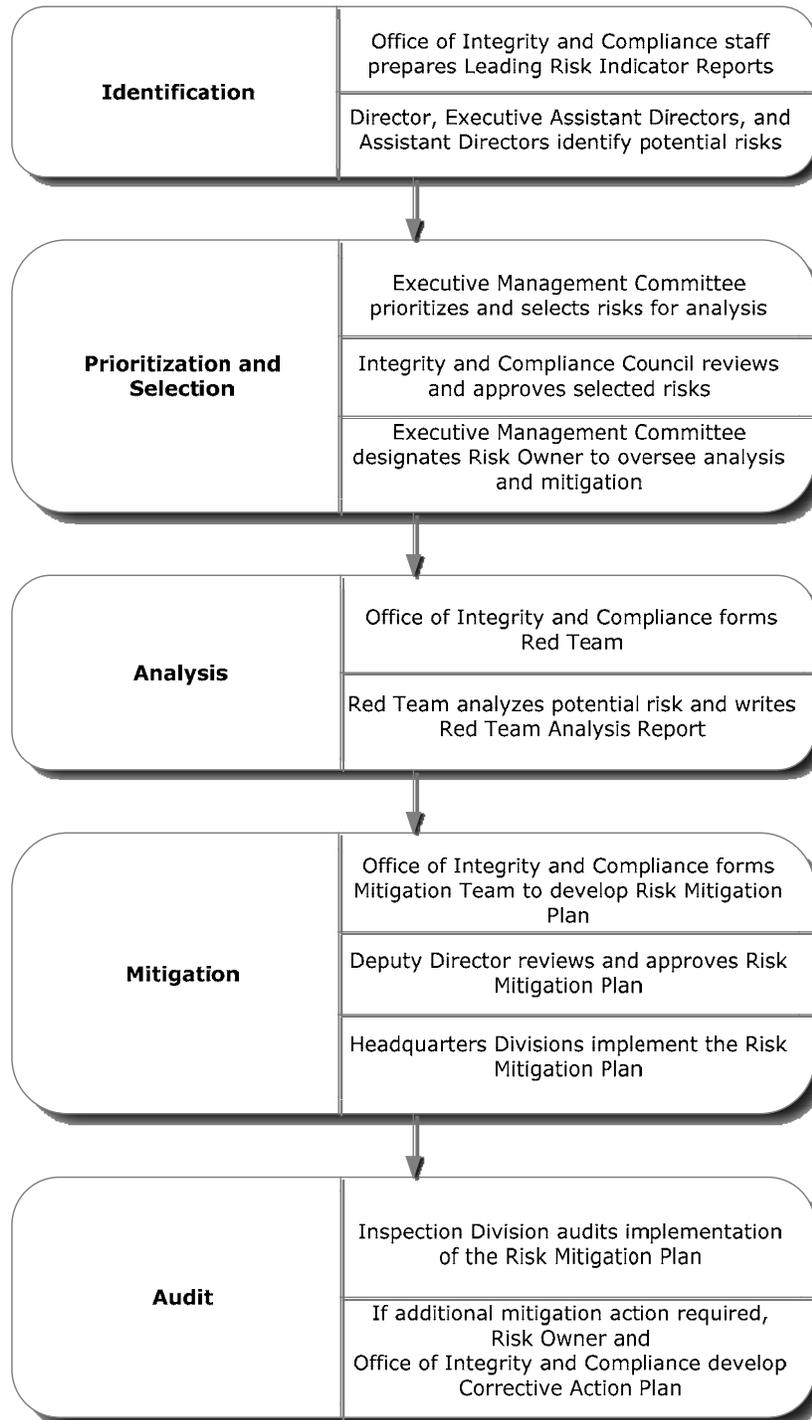
Executive Management Committee	Division
Administrative	Office of Equal Employment Opportunity Affairs
	Facilities and Logistics Services Division
	Finance Division
	Human Resources Division
	Inspection Division
	Office of Congressional Affairs
	Office of Law Enforcement Coordination
	Office of Public Affairs
	Office of Professional Responsibility
	Records Management Division
	Resource Planning Office
	Security Division
	Training Division
Criminal, Cyber, Response, and Services	Criminal Investigative Division
	Cyber Division
	Critical Incident Response Group
	International Operations Division
	Office of Victim Assistance
Information Technology	Office of the Chief Knowledge Officer
	Information Technology Engineering Division
	Information Technology Management Division
	Information Technology Operations Division
National Security	Counterintelligence Division
	Counterterrorism Division
	Directorate of Intelligence
	Weapons of Mass Destruction Directorate
Science and Technology	Criminal Justice information Services Division
	Laboratory Division
	Operational Technology Division

Source: FBI Organizational Chart.

There are five steps for addressing compliance risks at the FBI-wide level.

The FBI addresses compliance risks at the FBI-wide level in five steps: risk identification, risk prioritization and selection, risk analysis, risk mitigation, and audit. The process is displayed in Figure 1 and discussed below.

Figure 1: Risk Identification and Reduction of FBI-Wide Legal Compliance Risks



Source: OIG analysis of FBI program directives.

Risk Identification. The Director, Executive Assistant Directors, and Assistant Directors identify potential risks within their functional branch or division. The OIC also compiles summaries of potential legal compliance risks identified through its own research and from concerns reported by FBI employees. The OIC provides these summaries – known as Leading Risk Indicator Reports – to the Executive Management Committees to consider when they meet to prioritize and select new risks to analyze, tailoring the summaries to each of the committees’ subject areas. The Assistant Director of the OIC also ensures that committees select new risks to mitigate when the mitigation is complete for risks previously selected.

Risk Prioritization and Selection. After an Executive Management Committee identifies potential risks, it selects which ones to analyze. To assist the committee members in comparing and prioritizing risks based on a specific set of factors, the OIC created a risk assessment methodology based on the best practices of corporate compliance programs. To apply the methodology, participants determine a numeric score for each risk based on the frequency of the activity, consequence of non-compliance, and the probability of non-compliance. The first six factors below help determine the probability of non-compliance. The seventh factor helps determine the consequence of the activity. Participants also consider the potential for legal action and reputational harm to the FBI when assessing consequence.

1. *Complexity.* Does activity occur in multiple locations or internationally, involve external agencies, or have many legal requirements?
2. *Internal Risk Indicators.* Is there a history of compliance issues? Is there an existing process to assess risk in the area?
3. *External Risk Indicators.* Have other agencies had problems with the activity? Is there a trend in civil liability or overturned convictions, or external reports citing compliance issues?
4. *Environment.* Is the activity new or does it require new technology? Is there pressure to conduct the activity?
5. *Workforce.* Is there turnover among key personnel? Is the workforce experienced and adequately trained?
6. *Internal Work Process.* Is activity manual or automated? Does it allow individual discretion? Does it require approval and monitoring? Are responsibilities clearly defined?

7. *Impact on Privacy and Civil Liberties.* Does activity affect privacy, First Amendment rights, individuals directly, or other civil liberties?

The Executive Assistant Director for the committee approves the selection of the potential risk for analysis, and the Division considered to be most involved with the risk becomes responsible for analyzing the risk. The Assistant Director in charge of the selected division, or the Assistant Director's designee, becomes the "risk owner." The risk owner is responsible for overseeing the analysis. If the analysis shows that mitigation is needed, the risk owner is also responsible for overseeing the mitigation of the risk.

Risk Analysis. After the risk has been assigned to a risk owner, the risk owner forms a Red Team to analyze the selected risk. The Red Team, led by a representative from the division assigned to be the risk owner, assesses the adequacy of policies and procedures, training, and monitoring and auditing efforts associated with the risk, and identifies compliance weaknesses. The Red Team then produces a written report that includes a legal analysis of applicable law and regulations; and analysis of how existing policy and procedures, training, and monitoring and auditing efforts comply with the legal requirements outlined in the legal analysis. The Red Team also makes recommendations to address the weaknesses identified. Red Teams are usually composed of one or two OIC staff members, employees who are subject matter experts on the selected risk, and one attorney from the Office of General Counsel, who is responsible for writing the legal analysis. Red Teams typically have 90 days to complete their reports, but this deadline is largely dependent upon the complexity of the issue under review.

Risk Mitigation. If the Red Team's risk analysis determines that a legal compliance risk does exist, then a mitigation team is formed to design a plan to address the issues identified in the Red Team report. The mitigation team is led by a representative from the division assigned to be the risk owner. Mitigation team members are often the same as the Red Team's. If implementation of the mitigation plan requires technical expertise, then the OIC may request that the relevant division provide a representative with that expertise to the team. For example, if the mitigation requires the design of software, the OIC would request information technology specialists to assist the team. After the Deputy Director approves the mitigation plan, the divisions specified in the plan are then responsible for implementing the portions of the plan they are assigned.²⁶

²⁶ The OIC also can select and mitigate issues itself. For these issues, the OIC takes the place of the Red Team and the mitigation team.

Audit. When the ICP believes that a risk mitigation plan has been fully implemented, the OIC requests that the Inspection Division conduct an audit. The audit verifies whether the plan has been implemented, whether the risk of non-compliance is reduced, and whether there is non-compliance in the activity. The Inspection Division conducts its audit after enough time has passed for the implementation of the plan to reasonably have taken effect. If the audit determines that the risk was mitigated, the ICP closes the risk. If the audit shows that non-compliance risk remains, the risk owner, OIC staff, and relevant stakeholders will develop a corrective action plan until the risk has been fully mitigated.

On February 3, 2011, the FBI informally established a unit within the Inspection Division called the Compliance and Mitigation Unit. This unit was created to plan, design, and coordinate the audits of the implemented risk mitigation plans. The unit is led by a Section Chief and has four additional staff members. According to the FBI, as of August 2011 this unit had not been formally approved, but convenes regularly.

Risk Identification and Mitigation at the Program Level

At the program level, the FBI uses a different process to identify and mitigate legal compliance risks. FBI policy requires managers of 53 major programs to apply compliance principles and methodology to their programs to identify risks that can be mitigated within those programs.²⁷ The OIC determined which of the FBI's programs are "major" by reviewing budget data and consulting with the FBI's Inspection Division. FBI senior management reviewed and approved the list. These programs are located within headquarters divisions. See Appendix II for the list of FBI major programs.

Since June 2009, the OIC has required major program managers to identify and prioritize their top three legal compliance risks for mitigation and to submit reports twice a year to the OIC and their Assistant Directors. These reports are to include a description of these risks and the plan for mitigating the highest priority risk. The OIC reviews the program reports to make sure the issues identified are legal risks, the plans to address the risk are realistic, and that program managers are taking the steps that could reasonably be expected to reduce the risk. According to the template program managers use to develop risk mitigation plans, the program level should also include an audit or a way to monitor the mitigation steps.

²⁷ FBI Policy Directive 0126D, Application of the Integrity and Compliance Program to FBI Program Management, October 24, 2008.

Risk Identification within FBI Field Divisions

The FBI established the Division Compliance Officer position in 2007 to provide a single point of contact for each division in support of the ICP and to be the OIC's contact in each field division.²⁸ Twenty-seven headquarters divisions and all 56 field divisions have designated at least one individual to serve as their Division Compliance Officer.²⁹ In 84 percent of field divisions (47 of 56), the Division Compliance Officers are also the field divisions' Chief Division Counsels. In this capacity, the Division Compliance Officers provide advice and training regarding the legal and ethical requirements of the FBI.

In August 2011, the OIC submitted a draft policy to the FBI's Corporate Policy Office that would formally implement the ICP in field divisions. If approved, this policy will implement division compliance councils in each field division and will clarify the role of FBI employees serving as Division Compliance Officers. According to the policy, the councils will provide an additional level of risk identification and mitigation through which field divisions are to reduce legal compliance risks.

Purpose and Scope of the OIG's Review

The objectives of this review were to evaluate how the FBI's Integrity and Compliance Program: (1) identifies risks of non-compliance with laws, regulations, rules, and FBI and Department of Justice policies; (2) prioritizes and selects identified risks; (3) analyzes highly ranked risks; (4) mitigates risks with adequate corrective actions; (5) monitors the implementation of the corrective actions to ensure that mitigation is effective; and (6) promotes a culture of integrity and ethical compliance throughout the FBI.

We examined the FBI's ICP since its establishment in 2007 through August 2011, including the roles and responsibilities of all entities that are part of the program. We evaluated the program the FBI developed and implemented for risk identification, assessment, mitigation, and monitoring legal compliance risks FBI-wide and in major programs at the program level. Our methodology included in-person and telephone interviews of FBI personnel in the Washington, D.C., area, site visits to interview FBI field office personnel in three field divisions, reviewing a variety of documents such as FBI policies of the Integrity and Compliance Program and Executive Management Committee meeting minutes, administering an e-mail questionnaire for FBI major program

²⁸ FBI Policy Directive 0005D, FBI Division Compliance Officer, October 1, 2007.

²⁹ Four of the 56 field offices designated at least 2 people to be their Division Compliance Officers.

mangers, performing data analysis, and observing meetings of the Executive Management Committees. We conducted fieldwork from July 2010 to March 2011. More details on our methodology are discussed in Appendix III.

RESULTS OF THE REVIEW

THE ICP IS BEGINNING TO REDUCE THE FBI'S COMPLIANCE RISK

Through its ICP, the FBI has implemented strategies that have started to reduce legal compliance risk within FBI operations and activities. We found that, since the ICP's inception in 2007, the ICP has used a variety of sources to identify 206 FBI-wide potential risks and 112 program-level risks, and conducted risk analyses and developed mitigation plans. As a result, the FBI has started to reduce compliance risk by implementing mitigation plans for 13 FBI-wide risks and 16 program-level risks. Five of the implementations of FBI-wide plans have been audited, and we found that legal compliance risk was mitigated in three instances and not fully mitigated in two. Further, we determined that the process the ICP used to develop mitigation plans addressed the areas of compliance risk that the Red Teams identified in their risk analyses and involved relevant stakeholders. Finally, in managing the FBI's ethics program, the OIC has promoted reporting of compliance concerns.

The implementation of the ICP marked a fundamental change in how the FBI identifies and manages legal compliance risks before they develop into problems. Prior to the ICP, the FBI identified and addressed compliance risks unsystematically through efforts that were generally stove-piped within specific divisions. The ICP has improved FBI management's understanding of the FBI's compliance risks by requiring executives and managers to routinely and systematically identify risks. In addition, risk analyses and mitigation plans that the ICP developed at the FBI-wide level have the potential to reduce compliance risk because they incorporate the input of relevant stakeholders and subject matter experts within and outside of the FBI; address the adequacy of policy and procedure, training, and monitoring and auditing efforts; and, if necessary, propose significant operational and policy changes to address the identified risk.

At the FBI-wide level, we found that 3 of the 11 implemented mitigation plans that we reviewed mitigated compliance risk in their areas by implementing controls and operational and policy changes.³⁰ We found that two implemented mitigation plans had not mitigated the risk identified. The remaining six plans appeared reasonable, but we cannot conclude that they effectively reduced compliance risk because evidence for us to make such an assessment (such as an audit or mitigation action that we could observe in the field) was not available at the time our review. At the program level, we found that the ICP implemented 16 risk mitigation strategies. However, because there is no verification that the mitigation strategies were implemented and effective, we cannot conclude that compliance risk was mitigated in these areas.

The following two sections discuss the FBI's efforts to reduce legal compliance risk through the ICP in more detail.³¹

The ICP has identified risks using a variety of sources.

The ICP identifies legal compliance risks from a variety of sources at both the FBI-wide and the program level, as FBI policy requires.³² We interviewed 15 FBI executives, 3 from each of the 5 Executive Management Committees, and found that the variety of sources that they use to identify risks includes FBI executives; program managers; field division employees; and open source information such as policies, oversight entity reports, and newspaper articles.

The ICP uses a variety of sources to identify FBI-wide risks.

As of August 2011, the executives from the 5 Executive Management Committees, corresponding to the FBI's 5 functional branches, and OIC staff members had collectively identified approximately 206 potential risk indicators for consideration by the

³⁰ We did not review 2 of the 13 implemented mitigation plans because they contained classified material, and we determined that access to that material was not essential to our review.

³¹ The ICP is not a separate office within the FBI. Except for OIC staff members who manage the program full-time, the remaining work of the program is conducted by FBI employees and committees who do the work of the program in addition to their regular duties. In this report we attribute actions to the ICP to convey that various individuals or entities are collectively performing the ICP's functions.

³² FBI Policy Directive 0002D, FBI Integrity and Compliance Program, June 25, 2007.

Executive Management Committees.³³ Of these potential risks, FBI executives selected 50 for analysis. The five Executive Assistant Directors we interviewed described the way they identify risks within their branches as drawing on their own experience and expertise and consulting with their Assistant Directors, who they also require to identify risks within their divisions.

FBI executives told us that they use a variety of sources, as well as their general knowledge of their branches, to identify FBI-wide risks. Six of the 10 Assistant Directors we interviewed stated that they identify risks, in part, by consulting their staff members and talking to their employees who work in field divisions. For example, the Assistant Directors in charge of the Weapons of Mass Destruction Directorate and Operational Technology Division have employees from their programs embedded in field divisions. The positions of these employees allow them to become aware of issues affecting the field and also to report the concerns they identify to supervisors or compliance officers at headquarters. One Assistant Director told us that his Division Compliance officer solicits risks from his program coordinators in field divisions and that any risks identified are “rolled up” from the Unit Chiefs to the Section Chiefs, and then to him and the Executive Management Committees.³⁴ He provided an example of a legal risk being identified in the field (see text box).

Compliance Risk of FBI Employees Following Policy that Does Not Reflect Current Presidential Order

A Special Agent in Charge of a field office contacted a section chief in the Weapons of Mass Destruction Directorate at FBI headquarters after learning that a new presidential order made Immigration and Customs Enforcement the lead agency on weapons of mass destruction task forces. The Assistant Director of the Directorate told us he viewed this as a compliance risk for the FBI because if FBI employees adhered to the superseded policy, which assumed that the FBI was the lead agency, they could be out of compliance with the presidential order. He raised the issue to the Executive Assistant Director of the National Security Branch.

³³ Before Executive Management Committees review potential risks and determine whether they may be a concern for the FBI, the FBI considers them “potential risk indicators.” We generated this estimate of potential risk indicators from Executive Management Committee meeting minutes, a list of risks identified at the inception of the ICP, and from Leading Risk Indicator Reports from the beginning of the ICP through summer 2010.

³⁴ In 2007, the FBI appointed Division Compliance Officers within FBI headquarters and each field office to provide a point of contact for each office in support of the ICP.

To help in the identification of legal risks, the OIC provides Leading Risk Indicator Reports to FBI executives for those quarterly meetings in which they will select a new risk to analyze. These reports summarize the risks pertaining to each branch that OIC staff members compile from their research of open source information, government reports, and new regulations, and from risks that individual FBI employees and employee groups reported to the OIC. OIC staff members prepare separate reports for each Executive Management Committee that summarize the legal risks pertaining to each committee's subject area. We analyzed the sources identified in the reports the OIC prepared between 2008 and 2010 and found that the OIC provided FBI executives risks to consider that OIC staff identified from sources within and outside of the FBI.

FBI managers of major programs are an additional source for risk identification within their program areas.

FBI policy requires managers of the FBI's 53 major programs to identify legal compliance risk within their program areas across 20 divisions and all 5 of the FBI's functional branches.³⁵ In the sample of bi-annual reports program managers submitted to the OIC in December 2010, we found that managers collectively identified 112 program-level legal compliance risks. Program managers from all but 9 of the 53 programs submitted reports detailing their identified risks. The OIC exempted one program in the Administrative Branch from reporting because it had been recently added to the FBI's major program list and two programs in the Science and Technology Branch because their managers were assisting with mitigating FBI-wide risks. Six other programs did not submit reports. In such instances, the OIC follows up with the program managers and directs managers to identify and submit risks "in accordance with FBI policy" in their next bi-annual reports.

Identifying risks has increased senior management's understanding of the FBI's vulnerabilities.

Senior FBI executives we interviewed stated that the ICP facilitates the identification of weaknesses that could result in non-compliance. For example, in our interview with the FBI Director, he noted that in the FBI, there is a tendency to concentrate on the agency's mission, to keep moving full-speed ahead, and consequently the FBI does not always focus on the potential risks. He said that a benefit of the ICP has been

³⁵ FBI Policy Directive 0126D, Application of the Integrity and Compliance Program to FBI Program Management, October 24, 2008.

that it identifies “gaps and vulnerabilities” and that the ICP has equipped him with more knowledge about the compliance threats facing the FBI and given him more confidence that there is follow-up on issues that are identified. The FBI’s General Counsel stated that an organized, methodical way of looking at risk is new in the FBI and that the FBI’s culture is to not talk about problems, but rather to solve them yourself. She stated that the ICP prompted a change in culture because executives are now willing to say, “We have a problem with ‘x.’” A program manager reiterated this view in response to our survey, stating “the process provides for a logical analysis of legal compliance gaps.”

Through the ICP, the FBI has started to reduce legal compliance risk by conducting risk analyses and by developing and implementing mitigation plans.

With the development of risk analyses and mitigation plans at both the FBI-wide and program levels, and implementation of those plans, the FBI has started to reduce legal compliance risks. According to the FBI, the ICP developed 26 total risk mitigation plans to address identified risks. Since its inception, the ICP has fully implemented 13 of the 26 mitigation plans for FBI-wide risks, and 3 of the plans have fully mitigated the compliance risk identified.³⁶ We determined that the process the ICP used to develop mitigation plans at this level addressed the areas of compliance risk that the Red Teams identified in their risk analyses and involved relevant stakeholders. At the program level, our review of the reports that program managers submitted to the OIC covering mitigation work completed or initiated between December 2009 and July 2010 found that mitigation plans had been implemented for 102 risks and that OIC staff members had determined 16 of those risks to be closed and fully mitigated.

The following sections discuss the FBI’s efforts to reduce legal compliance risk through the ICP in more detail.

At the FBI-wide level, the ICP has started to reduce the risk of legal non-compliance by implementing mitigation plans.

The ICP mitigated the compliance risk identified in three FBI-wide areas. On the basis of two completed FBI Inspection Division audits that found the risks to be mitigated as well as one OIG audit, we conclude

³⁶ Our review only addressed the 13 plans that had been fully implemented at the time of our fieldwork.

that the FBI has reduced legal compliance risks in three areas. As an example, below we summarize one of three risks identified, the mitigation steps taken, and the results of the audit of the mitigation steps.

An analysis team evaluated various areas of vulnerability in the collection of and access to DNA information. One conclusion was that the delay in collecting, analyzing, and uploading DNA samples from federal convicted offenders, federal arrestees, and non-U.S. detainees to the Combined DNA Index System could lead to congressional inquiries, public criticism, and litigation from crime victims. The mitigation team developed a mitigation plan, dated January 24, 2008, to eliminate the existing Federal Convicted Offender Program backlog and minimize the probability of future backlogs by hiring additional staff and acquiring additional laboratory space and equipment. An OIG audit found that the FBI successfully eliminated this backlog and reduced the compliance risk in this area.³⁷

The ICP did not fully mitigate the identified risk in two FBI-wide areas. FBI Inspection Division audits of two other implemented mitigation plans found that the risks identified had not been fully mitigated. In response, as of August 2011, the ICP was developing and implementing corrective action plans as required by FBI policy. FBI policy states that that Integrity and Compliance Council members “shall review and assess the results of audits performed in connection with the ICP to determine whether additional corrective measures should be employed and make related recommendations.”³⁸ As an example, below we summarize one of the two risks identified, the mitigation steps taken, and the results of the audit of the mitigation steps.

FBI Special Agents can use administrative subpoenas to obtain information to support investigations involving controlled substances or the sexual exploitation or abuse of children. The ICP found that the process for obtaining administrative subpoenas allowed agents to use them for other types of investigations and that the FBI did not have a way to track the overall number of administrative subpoenas issued, as the Attorney General’s

³⁷ U.S. Department of Justice Office of the Inspector General, *Audit of the Federal Bureau of Investigation’s Convicted Offender, Arrestee, and Detainee DNA Backlog*, Audit Report 11-39 (September 2011), 19-21.

³⁸ FBI Policy Directive 0004D, FBI Integrity and Compliance Council Charter, June 25, 2007.

Guidelines require.³⁹ To mitigate this risk, the ICP developed a plan, dated October 11, 2007, to automate the form that agents use to request administrative subpoenas. The automated form was to include a built-in control that would limit the types of investigations for which agents could obtain administrative subpoenas. The automated system was also to track each request.

A March 2011 FBI Inspection Division audit of the mitigation steps found that compliance concerns remained and, as a result, the audit made 11 recommendations for further mitigation of the administrative subpoena compliance risk. As of August 2011, the ICP was developing a corrective action plan and expected to have a draft in early September 2011.

For these two risks to be mitigated, the corrective action plans must address the findings and recommendations of the audits and be implemented. Because in one case the corrective action plan has not yet been implemented, and in the other case the plan has not yet been developed, we conclude that these risks have not been fully mitigated.

Assessment is not yet possible for six FBI-wide risk areas. The ICP considers the mitigation plans for six risks to have been implemented. But at the time of our review, the mitigation actions for these risks had not been audited, and the changes were either not observable in the field or had not been implemented when we made our site visits. As a result, we cannot conclude that these risks have been mitigated. As an example, below we summarize one of these six risks and the mitigation actions proposed in the mitigation plan.

A confidential human source is an individual who provides intelligence to the FBI on FBI investigative and national intelligence priorities. A 2005 OIG report found instances of non-compliance with Attorney General Guidelines in the FBI's use of confidential human sources due to inadequate administrative support, failure to hold supervisors accountable for compliance deficiencies and to exercise effective oversight of agents using confidential informants, inadequate training on appropriate methods to operate confidential informants, and differences in FBI and Department informant

³⁹ The Attorney General's Guidelines for Domestic FBI Operations state that the FBI should maintain a database or records system that permits a prompt retrieval of the status and basis for each investigation.

policies.⁴⁰ Subsequent to the OIG report, the FBI formed analysis teams to address confidential human sources-related compliance risks. According to the FBI, as a result of the team findings, mitigation efforts were implemented to improve policy, procedures, and training affecting the control and use of confidential human sources in accordance with the OIG report and the analysis team recommendations.

We believe that if the ICP effectively implemented the actions as described in the plans for the six risks that have not yet been audited, it is reasonable to expect that the actions will reduce compliance risk in those areas. However, without verification that the actions were implemented and effectively addressed the compliance risks, we cannot reach a conclusion that risks were fully mitigated.

The ICP's process for developing mitigation plans includes relevant stakeholders and has resulted in the development of comprehensive mitigation plans. Our review of the ICP's process for developing FBI-wide mitigation plans found that they involved the participation of relevant stakeholders and subject matter experts within and outside the FBI.⁴¹ In addition, the mitigation process sometimes led to the creation of inter- and intra-agency working groups so that the mitigation plans were developed with the perspectives of the stakeholders and experts knowledgeable about the risk area. At least 3 FBI divisions participated in the mitigation of each FBI-wide risk, and in one case, 10 divisions participated. Two of the mitigation plans required the participation of more than one Executive Management Committee to address a technical aspect of the risk, one required an inter-agency working group, three required intra-agency working groups, and five required consultation and involvement with Department executive offices. The mitigation teams consult with Department executive offices, such as the Office of Legislative Affairs if a mitigation plan proposes statutory changes or the Criminal Division if a mitigation plan proposes changes that fall within that division's jurisdiction. FBI executives we interviewed stated that FBI-wide risk mitigation is effective and beneficial because it involves collaboration across FBI functional areas. For example, the FBI's General Counsel stated that through the ICP, everyone with a role comes

⁴⁰ U.S. Department of Justice Office of the Inspector General, *The FBI's Compliance with the Attorney General's Investigative Guidelines* (September 2005).

⁴¹ Mitigation plans are developed based on the findings of the Red Teams' risk analyses.

together, and the ICP “gets [them] rowing in the same direction at the same time.”

Our review of the mitigation plans also found that each contained elements to address relevant compliance weaknesses, as identified in the risk analysis. Specifically, 9 of the 11 plans proposed changes to existing FBI policy or that new policy be drafted, and 10 of the 11 identified the need for and recommended that existing training be modified or additional training be developed and implemented. The plans also proposed significant changes in operations to reduce compliance risk, including the design and deployment of new software and equipment, as well as changes to Department policy and federal legislation.

In addition to implementing mitigation plans for FBI-wide risks, the ICP has also implemented 16 program-level risks. We discuss these below.

At the program level, the ICP implemented mitigation strategies for 16 risks.

In our review of the reports that program managers submitted to the OIC covering their program-level risk mitigation work completed or initiated between December 2009 and July 2010, we found that program managers had identified a total of 112 risks.⁴² OIC staff determined that 16 risks had been closed and fully mitigated and that program managers had begun mitigating 86 additional risks. For the remaining 10 risks that managers identified, mitigation procedures had not begun. Because the ICP does not require independent verification of program-level mitigation actions to confirm that the actions were actually completed and effective, we cannot conclude that the actions reduced compliance risk in these areas. However, as we explain in more detail below, we note that the mitigation actions for 5 of the 16 risks that the OIC considered closed established internal controls that we believe could reasonably be expected to reduce the risk. In contrast, the remaining 11 risks did not provide for any monitoring of the mitigation actions and thus provided less assurance of effectiveness.

The mitigation actions for five program-level risks included either an internal audit or the implementation of an automated system that would reduce the likelihood of human error. We conclude that these controls

⁴² These are the risks mentioned in the reports we reviewed for one reporting cycle. If program-level risks were identified and mitigated in previous reports, they would not be included in this total.

appear reasonable to reduce compliance risk. As an example, below we discuss one of the five compliance risks and the controls program managers described in their report.

The Surveillance and Aviation Program mitigated a risk of non-compliance with the Federal Aviation Administration's requirements for pilot currency and safe aircraft operations. The program mitigated the risk by adding three new elements to the annual field division inspections that FBI instructor pilots conduct. Specifically, instructor pilots examine divisions' compliance with safety and security requirements, make sure pilots' training is up to date, and verify that field divisions comply with all FBI aviation procedures.

The OIC determined that 11 additional risks had been mitigated. For all 11 risks reviewed, we found that none included the implementation of a control or any kind of monitoring to help ensure ongoing compliance, nor did the program assess the effectiveness of the mitigation actions. For example, the National Name Check Program, which disseminates information from FBI files to other federal agencies when requested, identified a risk that an inadvertent release of protected information might occur. To mitigate the risk, the program developed a standard operating procedure. It also required all National Name Check Program employees to attend annual training covering the guidelines for disseminating certain information. However, other than the Quality Assurance Program that was already in place, which reviews about 10 percent of outgoing work, no monitoring was put into place to see if the training was successful or if the risk of inadvertent disclosure was addressed.

In some cases, there may be a monitoring mechanism in place, but in current practice existing monitoring or its results are not necessarily shared with the OIC. If the OIC is not aware of monitoring and the program does not report the results of monitoring efforts, there is still no way to ensure that the risk mitigation occurred and was effective. Without some kind of monitoring of the risk and verification that the actions stated in the mitigation plan were actually performed and resulted in the needed changes, it is not possible to know whether the steps were effective and actually reduced the risk.

The OIC manages the FBI's ethics program and promotes reporting of compliance concerns.

The OIC supports the ICP's objective of reducing compliance risk by promoting the reporting of compliance and ethical concerns within the FBI. The OIC does this by managing the FBI's Ethics and Standards of Conduct program (ethics program). The OIC also established human resource initiatives that encourage compliance and communication channels for FBI employees to report compliance concerns.

The OIC maintains and has enhanced the FBI's ethics program.

In 2007, the FBI transferred responsibility for maintaining the ethics program from the Office of General Counsel to the OIC. According to the *2008 State of the Integrity and Compliance Program* report, combining the ethics program with the OIC's compliance program allows the FBI to better coordinate and build on the experience of the personnel in both programs.

The OIC enhanced the ethics program by creating new ethics videos and creating and revising printed ethics information. The OIC created a video in 2008 to highlight the importance of the ICP that features the FBI Director and is shown as part of the new employee and in-service ethics training. Additionally, the OIC developed a video discussing and reinforcing the FBI's core values.⁴³ The OIC also created and distributed a brochure advising FBI employees to report compliance and ethics concerns to the OIC or the appropriate FBI headquarters division and revised the FBI Employee Ethics Handbook. OIC attorneys also receive calls and e-mails regarding ethics questions and provide legal opinions in response. For example, FBI employees contact the OIC for guidance regarding travel and the acceptance of gifts. One OIC attorney stated that in 1 year, he received and responded to more than 2,500 ethics questions.

⁴³ FBI core values are (1) rigorous obedience to the Constitution of the United States; (2) respect for the dignity of those we protect; (3) compassion; (4) fairness; (5) uncompromising personal integrity and institutional integrity; (6) accountability by accepting responsibility for our actions and decisions and the consequences of our actions and decisions; and (7) leadership, both personal and professional.

The FBI has established initiatives to encourage compliance and ethical behavior within the FBI.

The FBI supported the ICP by establishing human resource initiatives to encourage compliance and ethical behavior. In 2007, the FBI incorporated risk mitigation efforts into executive management's performance appraisals. In February 2008, the FBI established a non-retaliation policy that specifically prohibits retaliation against employees for reporting compliance concerns to support a work environment in which there is "open communication regarding compliance risks."⁴⁴ The FBI also established a Director's award to recognize outstanding employee contributions to the ICP and a Compliance Helpline to facilitate reporting of compliance concerns. Finally, in 2009, the FBI added an addendum to all FBI employee performance appraisals reminding employees to follow the guidelines outlined in the FBI Ethics and Integrity Program Manual and, in order to receive an outstanding rating, to support an environment in which co-workers understand the importance of and are comfortable raising compliance concerns.

To assess whether the FBI supported the intent of the ICP by not violating the retaliation policy, we examined all complaints of retaliation by FBI employees between January 2007 and February 2011. We found that in no case did an employee report a compliance concern to the OIC and later report retaliation for making that report.

To assess whether these initiatives were helping to encourage compliance and ethical behavior, we assessed whether FBI employees were aware of and receiving the Director's award the OIC established. We found that as of August 2011, 40 FBI employees had received the award since 2008, when the OIC first awarded it. Of those 40 employees, 35 were from headquarters and 5 were from the field divisions. During our field visits, we asked interviewees if they were aware of this award. We found that only 13 percent (8 of the 64) of field division employees we asked were aware of the award. While this is understandable given that the ICP has so far been a largely headquarters-centric program, as the ICP is further implemented in field divisions, the FBI should raise awareness about this award to field division employees.

Finally, we assessed whether FBI employees were aware of the Compliance Helpline that the OIC created to facilitate the direct reporting

⁴⁴ The FBI non-retaliation policy does not expand or contract any "whistleblower" protection that may be available to FBI employees pursuant to 5 U.S.C. § 2303 and Department of Justice regulations set out in 28 C.F.R. Part 27.

of compliance concerns by FBI employees. While the OIC established and began receiving calls over the Compliance Helpline in September 2008, we found that only 20 percent (14 of 70) of the field division employees we asked were aware of it. As of October 2010, the OIC had received 47 Helpline calls from FBI employees, of which 22 were from field division employees. Field division employees need to be aware of the Helpline's existence for it to be an effective way of reporting compliance concerns.

Conclusions and Recommendation

The FBI, through the ICP, has started to implement legal compliance risk reduction strategies within its operations and activities by identifying and mitigating risks before they become problems. As of August 2011, the ICP had identified 206 FBI-wide potential risk indicators and 112 program-level risks from a variety of sources, including FBI executives, program managers, employees, and open source information such as newspaper articles and government oversight reports. The ICP implemented mitigation plans for 13 FBI-wide risks and, according to the reports that program managers submitted to the OIC, 16 program-level risks. As of August 2011, we conclude that the ICP's implemented mitigation strategies reduced compliance risk in three FBI-wide risk areas.

The OIC also enhanced the ethics program by establishing initiatives to encourage compliance and ethical behavior within the FBI. However, we found that only 20 percent (14 of 70) of the field division employees we asked were aware of the Helpline the OIC established to facilitate direct reporting of compliance concerns and that only 13 percent (8 of the 64) of field division employees we asked were aware of the Director's award the OIC established to recognize contributions to the ICP.

For the ICP to increase its effectiveness in encouraging compliance and reporting of compliance concerns, we recommend that the FBI:

1. Increase employee awareness of the Compliance Helpline and other OIC human resource initiatives.

ADDRESSING AREAS FOR IMPROVEMENT COULD ENHANCE THE ICP'S EFFECTIVENESS

The FBI could improve the ICP's effectiveness and sustainability by addressing certain factors. We found that FBI executives and managers no longer consistently use the ICP's risk assessment methodology designed for the ICP to evaluate identified risks, and the risk assessment and selection process is unsystematic and undocumented. In addition, at the program level, there is no external verification that mitigation actions are complete and effective. Because of this lack of monitoring, the FBI cannot be sure that the ICP has successfully implemented the risk reduction strategies for the selected risks. Also, the ICP has not yet been fully implemented in field divisions, and as a result, field divisions' role in risk identification and reporting to the ICP is undeveloped. Finally, the OIC, which manages the ICP, has not established a way to evaluate the program's overall effectiveness or the effectiveness of its processes. Without evaluation, the ICP cannot identify where changes in the program should occur or ensure the sustainability of the ICP.

We identified areas for improvement in the ICP at both the FBI-wide and program levels involving the use of its risk assessment methodology, verification of risk mitigation strategies, and implementation of the ICP in field divisions. We discuss the areas for improvement and their impact on the effectiveness and sustainability of the ICP in the following sections.

FBI executives and managers are not using the ICP's risk assessment methodology, and the risk selection process is informal, unsystematic, and undocumented.

We found that executives and managers are making minimal use of the risk assessment methodology the FBI developed to assist them in applying their professional judgment to the assessment and selection of risks. The ICP does not require this tool to be used. The FBI based this methodology on its research of best practices in corporate compliance programs, and it reflects the factors the FBI deemed important in considering risks to be addressed through the ICP. To prioritize risks, participants calculate a numeric score for each risk based on the

frequency of the activity, the probability of non-compliance, and the consequence of non-compliance. The risk assessment methodology uses seven factors that we described in the background section of this report. The first six factors help calculate the probability of non-compliance. These factors are: complexity, internal risk indicators, external risk indicators, environment, workforce, and internal work process. The seventh factor, impact on privacy and civil liberties, helps determine the consequence of the activity. Participants also consider potential for legal action and reputational harm to the FBI when calculating consequence.

At the FBI-wide level, we found that as of fall 2010, FBI executives no longer consistently used the risk assessment methodology. Instead, ICP participants use their own, ad hoc criteria to prioritize risks. Interviewees from four of five Executive Management Committees told us that they did not use the methodology at all, and that they assessed risk through informal discussion before and during the quarterly Executive Management Committee meetings. Interviewees in the fifth Executive Management Committee told us that certain members of their committee sometimes used the FBI's methodology.⁴⁵ The criteria most of the executives used included overall impact or seriousness, protecting the reputation of the FBI, the availability of human resources to work on mitigating the risk, the probability of the risk's occurrence, the scope of the risk, negative financial impact, asking "what happens if we do nothing," and "what would we not want to read in the paper." While these are reasonable and important considerations – and many of them are incorporated into the risk assessment methodology – the FBI's current practices do not ensure that managers will consider them consistently. The Executive Management Committees' risk prioritization and selection are also not documented. While an attendee at each Executive Management Committee meeting takes minutes that include updates about the mitigation actions for risks undergoing mitigation, the minutes do not document how participants prioritized or selected risks for analysis.

Similarly, at the program level, we found that program managers' use of the methodology was limited. Based on our survey results of program managers, we concluded that program managers used their professional judgment alone to assess risk more often than the methodology. Only 29 percent (13 out of 45) of the managers who responded to our survey reported using the methodology or the criteria in

⁴⁵ We interviewed 15 FBI executives, 3 from each of the 5 Executive Management Committees.

it to select risks when asked, “What do you use to determine the legal compliance risk to mitigate?” The remaining 71 percent (32 out of 45) gave a variety of answers that did not coincide with use of the methodology. While professional judgment is essential, its value to the process can be increased if it is focused through the FBI’s risk assessment methodology. We found that program managers describe the risks they have identified and their plans to mitigate them in written reports to the OIC, but these reports do not explain why they chose one risk over another or document the relative significance of the risks. Program risk identification relies primarily on written communication with the OIC two times per year and does not require in-person contact between OIC staff members and managers. This sporadic involvement may not allow for sufficient understanding among program managers of how risks should be assessed and selected.

We believe that use of a risk methodology does not exclude the use of professional judgment and knowledge in making the assessment; rather, it enhances the use of professional judgment. Further, when FBI executives and managers do not use the risk assessment tool, they cannot demonstrate that they considered each risk against the factors the FBI considers important. For example, one of the factors used in the methodology to assess the significance of a risk’s consequence is its impact on privacy and civil liberties. In fact, FBI violations of privacy and civil liberties in its use of National Security Letter authority were what prompted the FBI to establish the ICP.⁴⁶ However, only 33 percent (5 of 15) of the executives we interviewed said they considered this factor when they made their assessments. The other 10 may have also considered this factor, but they did not articulate that to us when we asked them what factors they considered when assessing risks. Using a formal methodology would give consistency to risk assessment and selection by ensuring that current and future participants consider the criteria the FBI deems important when assessing risk. This is an important consideration because the ICP’s participants are unlikely to remain constant due to turnover within the FBI and the FBI plans to expand the ICP to include more FBI field division participation.

⁴⁶ U.S. Department of Justice Office of the Inspector General, *Review of the Federal Bureau of Investigation’s Use of National Security Letters* (March 9, 2007).

The ICP does not require external verification for major program mitigation efforts, and the OIC lacks the authority to require program-level participation

At the program level, we found that the ICP lacks a way to ensure that risk reduction strategies are implemented and that they are effective at reducing compliance risks. First, program-level mitigation does not include any independent assessment of implemented strategies. Because of this lack of follow-through, the FBI cannot be sure that the mitigation steps were implemented and that compliance risk was reduced. Second, OIC staff oversees the program-level risk mitigation, but does not have the authority to require program managers to participate. We found that six program managers did not participate as mandated by FBI policy.

In our sample of the reports that program managers submitted to the OIC covering activities completed, ongoing, or initiated from January through June 2010, we found that no mitigation actions were verified by an independent group, such as the FBI Inspection Division, individuals from another division, or even the OIC. We saw 24 instances in the sample where OIC staff members asked program managers to provide information about audit, monitoring, or “perceived effectiveness” of risk mitigation efforts, indicating that the OIC intended to use information about how well risk reduction strategies worked in its assessment. However, in no case did a program have an external verification to ensure that the mitigation actions had been taken and to assess the effectiveness of those actions. Verification could be as simple as someone checking that the plan is implemented and operational, and that the risk appears to be mitigated. Without this step, the ICP cannot ensure that managers’ mitigation actions are complete or effective.

While FBI policy mandates major program managers’ participation in the ICP, we found that this did not always occur.⁴⁷ Specifically, 6 of 53 programs did not submit written reports to the OIC, as required. In these instances, the OIC directed managers to identify and submit risks “in accordance with FBI policy” in their next bi-annual reports. OIC staff members manage program-level risk mitigation but do not have authority to require programs to participate. Assistant Directors could ensure that managers participate, but in our interviews only one of nine Assistant Directors we asked about program-level risk mitigation told us that he was aware of it, even though all nine were included in the distribution

⁴⁷ FBI Policy Directive 0126D, Application of the Integrity and Compliance Program to FBI Program Management, October 24, 2008.

list for the reports about the risk mitigation activities. Moreover, the one Assistant Director who was aware of program-level risk mitigation questioned its value.

We believe that success at the program level depends not only on the work of program managers and OIC staff, but also the Assistant Directors' involvement and buy-in. Unlike the FBI-wide level of risk identification and mitigation, where senior executives meet quarterly with the OIC and the progress about risks is reported monthly to the FBI Director, at the program level, managers work more independently, often without any in-person interaction with OIC staff members. Program managers submit their reports to OIC staff members two times per year, and then the OIC staff review and provide feedback to the program managers. The Assistant Directors are included on the distribution lists for the reports from program managers to the OIC and then from the OIC to program managers, but their participation is not required.

For program-level risk mitigation to be an effective tool for reducing compliance risk, it should include verification that the mitigation actions were taken and are effective. The verifications should examine the risk mitigation efforts and make a determination about whether compliance risk was reduced. In addition, involving Assistant Directors would ensure that they were aware of the risks their managers were addressing and that program managers prioritized program-level risk mitigation.

The ICP is not fully implemented in field divisions.

Although the majority of the ICP's risk identification and mitigation activities currently take place at FBI headquarters, the OIC intends for field division employees to play a role in identifying compliance concerns. The ICP plans to establish field division compliance councils that will identify and mitigate risks, and has established a Division Compliance Officer position within field divisions to coordinate each field division's council. However, the focus of the ICP thus far has been to implement the program at headquarters, and no formal structure has been established yet to implement the ICP in FBI field divisions.

In response to the 2007 creation of the Division Compliance Officer position, field divisions appointed officers, but as of fall 2010, the OIC had not fully developed or utilized this position, and the OIC's Assistant Director described it as "a latent role." The three Division Compliance Officers we interviewed in the field divisions we visited stated that they did not yet perform any additional tasks because of that role. They told us that, as their divisions' Chief Division Counsels, they already

performed most the duties that the Division Compliance Officer policy established, such as providing legal and ethics advice and ethics training to FBI employees.⁴⁸ The one duty that these three Division Compliance Officers did not currently perform was coordination with the OIC.

Additionally, as of August 2011 the ICP had not established a method to identify and mitigate compliance risks in field divisions. What we observed in 2010 seemed largely unchanged from the OIC's assessment in 2008 when it wrote in the *State of the Integrity and Compliance Program* report that the "compliance portion of the program is still relatively unheralded beyond headquarters." We found that field division employees were more likely to report compliance concerns to officials within their field divisions rather than to the OIC. During our site visit interviews, field division employees told us that they preferred to handle issues within their field divisions rather than to involve headquarters. Seventy of the 75 field division employees we interviewed told us that when they have a legal or a compliance-related question, they seek assistance from their Chief Division Counsels first. All three field Chief Division Counsels we interviewed (who also served as their field divisions' Division Compliance Officers) indicated they would resolve issues within the field division if possible. While resolving issues at the lowest possible level is generally preferable, if potential legal compliance issues are not consistently reported to the OIC – even if they are solved at the field division level – broader issues may not be recognized.

In August 2011 the OIC's Assistant Director submitted a draft policy to the FBI's Corporate Policy Office that would formally implement the ICP in field divisions. This policy would require each field division to establish a compliance council that would be required to meet at least twice a year. These councils would identify potential compliance risks and determine whether they constitute actual compliance risk within the division. For risks identified that pose a compliance risk within the division, the council would develop, implement, and track to completion mitigation plans. The council would inform the OIC of FBI-wide compliance risks and risks that could affect multiple field divisions. This policy would clarify the role of the Division Compliance Officer and require the Division Compliance Officer to be a field division senior manager "not lower than an Assistant Special Agent in Charge" because "for the ICP to succeed in the field, the ICP point of contact needs to have a certain level of authority." Assistant Special Agents in Charge have

⁴⁸ In 47 of 56 of field offices the Chief Division Counsel serves as the Division Compliance Officer.

more authority than Chief Division Counsels. Although they will no longer serve as Division Compliance Officers, the Chief Division Counsels would continue to administer the field divisions' ethics program, provide legal advice, and respond to compliance concerns. The Division Compliance Officer would lead the compliance council whose membership would include the Chief Division Counsel and other field division staff.

Having input from field divisions will help the ICP have a complete picture of compliance risks in FBI operations. Ten of 15 FBI executives we interviewed stated that field input to the ICP was important.⁴⁹ One Executive Assistant Director stated that he wanted "risks to come from everyone because there may be additional perspectives or perceived risks." Similarly, the FBI's General Counsel stated that she expected the ICP would be getting field input because "we operate in the field" and "risks exist in the field." Because field division employees are more likely to report compliance concerns to officials within their field division rather than to headquarters, the effectiveness of the ICP's efforts to ensure that risks identified in the field are reported to the ICP depends on the development of the ICP in field divisions.

The OIC has not established a way to assess the ICP's overall effectiveness or to measure progress toward achievement of ICP goals.

While the OIC is responsible for assessing the ICP, it has not evaluated the effectiveness of the ICP's risk identification and mitigation efforts at either the FBI-wide or program level nor has it measured its progress toward achievement of the ICP's goals since 2008. The OIC has not created the annual report of the ICP's activities that FBI policy requires since 2008, and it does not track the ICP's progress toward attaining the program's goals. The OIC's tool for measuring the FBI's culture of compliance does not substitute as a way to measure the performance of the ICP. Without a way to assess the ICP and a way to measure progress toward accomplishment of the ICP's goals, the OIC cannot determine the ICP's effectiveness at reducing compliance risk or identify where changes in the program should occur to ensure the sustainability of the ICP.

The 2008 report summarized the elements of the ICP, the goals of the ICP, the steps the OIC took or planned to take to accomplish the

⁴⁹ The other five executives may consider field input important but did not specifically state that during interviews.

ICP's goals, and assessed how the ICP was doing so far.⁵⁰ According to the OIC's Assistant Director, the report was discontinued because it was too time consuming to write and duplicative of a monthly report that the OIC prepared for the FBI Director. This monthly report shows the status of all FBI-wide risks the ICP is mitigating, the degree to which the ICP has implemented each mitigation plan, and whether it considers any part of the mitigation process to be delayed. However, the monthly report does not provide information about the status of program-level risks, overall accomplishments of the ICP, challenges to the ICP, or information about whether the ICP is accomplishing its goals or future plans.

The OIC Assistant Director told us that the ICP uses responses to ethics- and integrity-related questions on the FBI's employee survey to assess the FBI's culture of compliance (see Appendix V). While the survey data provides a useful assessment of the culture of compliance, it does not provide an adequate assessment of the ICP's performance. While the efforts of the ICP may contribute to the positive ethical climate and culture of compliance, the survey cannot distill what aspects of the culture of compliance are attributable to the ICP's efforts, as opposed to other activities in the FBI. It is not possible to know whether or to what degree the ICP's activities have affected the culture based on the survey because the survey results have been consistently high year after year and were already high at the time of the creation of the ICP. An FBI survey analyst told us that the data over 3 years does not show any statistically significant trends.

While it is difficult to objectively evaluate the ICP, we believe the OIC could evaluate the extent to which the ICP effected shifts in the FBI's culture of compliance and changes in how the FBI manages compliance risk. A consolidated annual report similar to the FBI's *2008 State of the Integrity and Compliance Program* report would be a tool for FBI executives and OIC management to gauge the ICP's effectiveness; to review progress toward completing planned activities, strengths of, and challenges to the program; would increase awareness about the ICP; and would show what impact the ICP has had on the FBI.

Conclusions and Recommendations

We identified areas for improvement in the ICP at both the FBI-wide and program levels that, if addressed, could enhance its

⁵⁰ The ICP goals are described as strategic shifts. These are summarized in Appendix IV.

effectiveness and sustainability. We found that FBI executives and managers do not use the risk assessment methodology designed for the ICP to evaluate identified risks and that risk assessment and selection is unsystematic and undocumented. The FBI cannot address all potential risks simultaneously because each risk requires significant resources to analyze and mitigate. Thus, it is important that the ICP produce a common understanding of risks' relative priority so that executives and managers select those potential risks that most closely align with the criteria contained in the risk assessment methodology.

In addition, at the program level, the ICP does not have external verification nor is it able to ensure full participation by major programs. Because of this lack of external verification and because there is a lack of involvement by officials with the authority to require program manager participation, the FBI cannot be sure that the ICP has successfully implemented the mitigation actions for the selected risks.

Also, the OIC has not yet fully implemented the ICP in field divisions, and as a result, field divisions' role in risk identification and reporting to the OIC is undeveloped. Finally, the OIC has not established a way to evaluate the ICP's overall effectiveness or the effectiveness of its processes. Without this, the FBI cannot identify where changes in the ICP should occur and ensure the sustainability of the program.

To ensure the sustainability and improve the effectiveness of the ICP, we recommend that the FBI:

2. Consider using a formal methodology that includes specific criteria that participants must consider when assessing and prioritizing risk.
3. Increase Assistant Director involvement in program-level risk mitigation.
4. Require program-level risks to include a verification step.
5. Comply with existing requirements for an annual report assessing the effectiveness of the ICP, for example, a report that articulates the program's goals, shows progress toward accomplishing them, and identifies areas for improvement.

CONCLUSION AND RECOMMENDATIONS

We conclude that the FBI, through the ICP, has started to reduce the FBI's risk of legal non-compliance and that the ICP has the potential to further reduce risk by identifying risks and making the operational and policy changes necessary to mitigate them before they become problems. As of August 2011, the ICP's implemented mitigation strategies reduced compliance risk in three FBI-wide risk areas. Further, the ICP improved the FBI's ability to identify its potential compliance risks by, for example, using a variety of sources to identify potential risks. We believe that the concept of the FBI's OIC program has been beneficial to its efforts to monitor and enhance compliance with legal requirements, and that other agencies may wish to consider implementing a similar kind of program. We found that the ICP's process for developing mitigation strategies resulted in comprehensive plans that, if implemented as described, we believe would reduce compliance risk in those areas.

We identified several areas in the ICP that, if refined, could improve the ICP's ability to reduce legal compliance risk and the ICP's sustainability. The OIC manages the FBI's ethics program and promotes reporting of compliance concerns, and has enhanced the program by establishing new initiatives to encourage compliance and ethical behavior within the FBI. However, we found that only 20 percent (14 of 70) of the field division employees we asked were aware of the Helpline the OIC established to facilitate direct reporting of compliance concerns. Only 13 percent (8 of the 64) of field division employees we asked were aware of the Director's award the OIC established to recognize contributions to the ICP. For these initiatives to be effective, FBI personnel must be aware of them.

In addition, we found that FBI executives and managers do not use the risk assessment methodology designed for the ICP to prioritize identified risks and that risk prioritization and selection is informal, unsystematic, and undocumented. It is important for the ICP to produce a common understanding of risks' relative priority so that executives and managers select, analyze, and mitigate those that most closely align with the criteria contained in the risk assessment methodology.

Further, at the program level there is no external verification that mitigation actions were completed and were effective. Because of this lack of monitoring, the FBI cannot be sure that the ICP successfully implemented the mitigation actions for the identified risks.

Also, the OIC has not yet fully implemented the ICP in field divisions, and as a result, field divisions' role in risk identification and reporting to the OIC is undeveloped. Finally, the OIC has not established a way to evaluate the ICP's overall effectiveness or the effectiveness of its processes. Without this, the FBI cannot identify where changes in the ICP should occur and ensure the sustainability of the program.

To ensure the sustainability and improve the effectiveness of the ICP, we recommend that the FBI:

1. Increase awareness of the Compliance Helpline and other OIC human resource initiatives.
2. Consider using a formal methodology that includes specific criteria that participants must consider when assessing and prioritizing risk.
3. Increase Assistant Director involvement in program-level risk mitigation.
4. Require program-level risks to include a verification step.
5. Comply with existing requirements for an annual report assessing the effectiveness of the ICP, for example, a report that articulates the program's goals, shows progress toward accomplishing them, and identifies areas for improvement.

APPENDIX I: FBI COMPLIANCE PROGRAM POLICIES

FBI Corporate Policy	Date Approved	Summary
Integrity and Compliance Program, 0002D	June 25, 2007	Establishes the Integrity and Compliance Program and the Office of Integrity and Compliance and describes their responsibilities. Additionally, it explains the roles of the Inspection Division and the Office of General Counsel in the Integrity and Compliance Program.
Integrity and Compliance Executive Management Committees Charter, 0003D	June 25, 2007	Describes the membership of each Executive Management Committee, and the membership's roles and responsibilities in the Integrity and Compliance Program.
Integrity and Compliance Council Charter, 0004D	June 25, 2007	Details the purpose of the Integrity and Compliance Council, its members, and the members' roles and responsibilities.
Division Compliance Officer, 0005D	October 1, 2007	States that each division must appoint a Division Compliance Officer. This policy establishes that the Division Compliance Officer, which is a collateral duty, is to provide a single point of contact for each field division.
Executive Performance Appraisals - Compliance, 0006D	October 1, 2007	Integrates the Integrity and Compliance Program into executive management performance appraisals. Specifically, it requires that FBI executive management review and mitigate each of the number-one compliance risks identified by the five Executive Management Committees.
Non-Retaliation for Reporting Compliance Risks, 0032D	February 11, 2008	States that FBI management shall train their personnel on ways to report compliance risks. It also encourages employees to report compliance concerns, and prohibits retaliation against anyone who reports them.
Application of the Integrity and Compliance Program to FBI Program Management, 0126D	October 24, 2008	Identifies the FBI programs the Integrity and Compliance Program considers "major." In addition, this directive states that major programs must prioritize their top three risks and mitigate them one at a time in order of priority.
Compliance Risk Referrals, 0136D	October 24, 2008	Describes the process the Office of Integrity and Compliance must follow when compliance risks are reported.

APPENDIX II: LIST OF FBI MAJOR PROGRAMS

1. Facilities Management and Acquisition Program
2. Fleet Management & Transportation Services Program
3. Secure Work Environment Program
4. Applicant Program
5. Executive Development & Selection Program
6. Healthcare/Medical Services Program
7. Human Resource Information Systems Program
8. Human Resources Management Program
9. Freedom of Information Privacy Acts Program
10. National Name Check Program
11. Information Assurance Program
12. Personnel Security Program
13. Training Program
14. Defensive Systems Program
15. Civil Rights Program
16. Gang/Criminal Enterprise Program
17. Organized Crime Program
18. Public Corruption/Civil Rights Program
19. Undercover and Sensitive Ops Program
20. Violent Crimes Program
21. Financial Crimes Section/Health Care Fraud
22. Critical Incident Response Program
23. Surveillance and Aviation Program
24. Computer Intrusion Program
25. Cyber Crime Program
26. Legat Attaché Program
27. IT Engineering Program
28. IT Management Program
29. IT Services Program
30. Knowledge Management Program
31. Counterintelligence Program
32. Domestic Terrorism Program
33. International Terrorism Program
34. Foreign Terrorist Tracking Taskforce Program
35. Foreign Language Program
36. Human Intelligence Program
37. Intelligence Program
38. Weapons of Mass Destruction
39. Biometric Interoperability Program
40. IAFIS/Interoperability Program
41. Law Enforcement National Data Exchange Program

-
42. Next Generation Identification Program
 43. Biometrics (Biometric Center of Excellence) Program
 44. Combined DNA Index System Program
 45. Field Evidence Program
 46. Operational Response Program
 47. Advanced Electronic Surveillance and Search Program
 48. Digital Evidence Forensics Program
 49. Radio Program
 50. Specialized Support and Coordination Program
 51. Tactical Operations Program
 52. Technical Personnel and Defensive Program
 53. Video Physical Surveillance Program

APPENDIX III: METHODOLOGY OF THE OIG REVIEW

We conducted in-person and telephone interviews of FBI personnel in the Washington, D.C., area, conducted site visits to interview field division personnel, and reviewed policies of the Integrity and Compliance Program. We conducted document reviews, performed data analysis, observed meetings of the Executive Management Committees, and attended an Ethics and Compliance Officers Association’s annual conference. We also developed an e-mail survey for FBI program managers.

Interviews

We interviewed 118 FBI officials and staff members at headquarters and field divisions, and 3 non-FBI personnel. The 37 FBI headquarters-level interviews provided information on the overall operations of the ICP. Of the 118 interviews of FBI staff, 81 were conducted at field divisions and provided insight into the current level of field involvement in and awareness of the ICP. We conducted the three non-FBI interviews to learn about corporate compliance programs. See below for a list of officials interviewed during the review.

Organization	Interviewees by Position
Integrity and Compliance Council & Executive Management Committee Participants	FBI Director
	Associate Deputy Director (former Executive Assistant Director, Criminal, Cyber, Response and Services Branch)
	Executive Assistant Director, National Security Branch
	Executive Assistant Director, Science & Technology Branch
	Executive Assistant Director, Information Technology Branch
	Executive Assistant Director, Human Resources Branch
	General Counsel
	Assistant Director, Criminal Investigative Division
	Assistant Director, Information Technology
	Assistant Director, Directorate of Intelligence
	Assistant Director, Critical Incident Response Group
	Assistant Director, Operational Technology Division
	Assistant Director, Weapons of Mass Destruction Directorate
	Assistant Director, Human Resources Division
	Section Chief, Special Technologies and Applications Office
Chief Knowledge Officer	
Deputy Assistant Director, Training Division	

Organization	Interviewees by Position
Office of Integrity and Compliance	Assistant Director, Office of Integrity and Compliance
	1 Unit Chief
	9 Attorneys
	1 Supervisory Special Agent
	2 Management Analysts
Inspection Division	Assistant Director, Inspection Division
	Deputy Assistant Director, Inspection Division
	Section Chief, External Audit and Compliance, Inspection Division
	Chief Inspector, Inspection Division
Other FBI Personnel	Chair, Middle Management Committee
	Unit Chief, Criminal Investigative Division
Field Division Personnel	In the Knoxville Field Division, we interviewed the Special Agent in Charge, the Chief Division Counsel (serves as the Division Compliance Officer), and 17 other staff consisting of Assistant Special Agents in Charge; Supervisory Special Agents; Special Agents; Intelligence Analysts; Technical Information Specialists; a Support Supervisor; and an Auditor.
	In the Sacramento Field Division, we interviewed the Special Agent in Charge, the Chief Division Counsel (serves as the Division Compliance Officer), and 30 other staff consisting of Assistant Special Agents in Charge; Supervisory Special Agents; Special Agents; Intelligence Analysts; a Support Services Technician; a Supervisory Administrative Specialist; a Victim Specialist; an Investigative Operations Analyst; a Electronic Surveillance Technician; and an Auditor.
	In the Miami Field Division, we interviewed the Special Agent in Charge, the Chief Division Counsel (serves as the Division Compliance Officer), and 28 other staff consisting of Assistant Special Agents in Charge; Supervisory Special Agents; Special Agents; Intelligence Operations Specialists; a Supervisory Intelligence Analyst; a Support Operations Specialist; and a Support Supervisor.
Non-FBI Interviewees	Chief Executive Officer, Society of Corporate Compliance and Ethics
	Consultant to the FBI's Office of Integrity and Compliance
	Special Agent, Investigations Division, Office of the Inspector General

Site Visits

To assess the perspectives of field employees, we conducted site visits to the FBI's Knoxville, Miami, and Sacramento field divisions and interviewed employees about identifying and reporting compliance risks. We selected these field divisions based on a series of criteria, such as size of the office, type of investigation, and field office scores on FBI employee survey questions that the OIG added to assess the culture of compliance.

Document Reviews and Data Analyses

To determine the scope of the ICP and to understand how it functions, we reviewed policy directives governing the ICP, OIC brochures, information about ICP awards, and who has received them, routine directives from the OIC to field divisions, and FBI ethics materials. We also examined documentation from the ICP's risk identification, mitigation, and audit process including Integrity and Compliance Council and Executive Management Committee meeting minutes; risk analyses, mitigation plans, and audits; and program-level reports. To gain information about the program-level process for assessing and selecting risk we surveyed program managers from the FBI's major program areas and performed qualitative analyses of their responses. We also reviewed FBI's Inspection Division self-inspection reports for the FBI field divisions we visited to determine how these reports could be used in risk identification.

We analyzed Leading Risk Indicator Reports from 2008 through 2010 to determine what sources the ICP used in identifying potential risks, reviewed compliance concerns reported to the OIC via its Helpline and other sources to determine whether FBI employees were reporting compliance concerns to the ICP, and compared reports of compliance concerns against reports of retaliation to determine whether any employee was retaliated against for reporting a compliance concern. We also examined results from the FBI's 2007, 2008, and 2009 climate survey to assess whether a culture of compliance existed within the FBI.

To understand how program managers of the FBI's major programs participated in the ICP, we reviewed a sample of FBI program manager reports covering activities initiated or completed between December 2009 and June 2010. These reports included information from 53 programs about risks being identified and mitigated, and OIC feedback about the information program managers submitted.

Observations

To see the ICP process firsthand, we observed meetings of three Executive Management Committees in July 2010. In addition, we attended the Ethics and Compliance Officers Association's annual conference in September 2010 to gain a greater understanding of corporate compliance programs upon which the FBI's ICP is based.

Program Manager Survey

To learn more about how the ICP was implemented at the program level, we developed a nine-question e-mail survey for FBI program managers. The questions included the number of risks program managers had identified, the criteria used to identify risk, and ways the program benefitted them as well as any suggestions program managers had regarding the ICP process. We distributed the survey to 54 FBI program managers or their designees in the FBI's 53 major programs, and 48 managers responded representing 49 programs.⁵¹

⁵¹ Some major programs had more than one program manager, and six program managers that responded represented more than one program.

APPENDIX IV: FBI STRATEGIC SHIFTS ANTICIPATED BY OIC

**The Strategic Shifts the OIC Anticipated from
Implementation of the ICP**

Pre-ICP Establishment	Post-ICP Establishment
Cultural Changes in Views About Compliance Risk	
Compliance is viewed as an obstacle to mission accomplishment	Compliance is viewed as integral to mission accomplishment, and is incorporated into day-to-day operations, decision making and work processes
Compliance is a senior leadership concern only	Employees know and understand laws and policies of their work, ask questions, and report non compliance Managers teach employees rules
Non-compliance is enforced through punitive measures	Employees comfortable with raising compliance concerns Managers do not retaliate for and act on reports of non-compliance
Performance evaluation based on inspection and audit findings	Performance evaluation based on ability to identify programs, practices, and activities that may pose risks, determine causes of future failure points and mitigate those risks
Structural Changes in Managing Compliance Risk	
Scope is periodic, limited to certain programs, and reactive and backward looking	Scope is continuous, enterprise-wide, and proactive and forward looking
Internal communications are reactive, diffused, difficult to find, top-down	Internal communications are proactive, enterprise-wide, unified, easily accessible and top down and bottom-up
Risk identification stove-piped and primarily located in Inspection Division	Risk identification and mitigation at all levels and divisions
Mitigation is ad hoc and reactive	Formal structure with oversight
Conducted as collateral duty	Conducted by a cadre of full time compliance professionals
Resources are allocated in reaction to compliance issues	Resource requests and allocations are driven by risk identification, prioritization and mitigation

Note: The “strategic shifts” are an articulation of the ICP’s goals. These goals are changes in the way the FBI views and manages compliance as a result of the ICP.

Source: The FBI’s *2008 State of the Integrity and Compliance Program* report.

APPENDIX V: FBI EMPLOYEE SURVEY QUESTIONS

Employee Survey Question	2007	2008	2009
Following the law is just as important as accomplishing the mission	4.54	4.56	4.73
If my supervisor tells me to ignore a minor procedure established by laws, regulations or policies, I assume he or she has a good reason and will follow orders without asking for those reasons	3.91	3.95	4.09
Sometimes it is necessary for me to ignore the literal requirements of a law, regulation or policy to meet the FBI mission	4.02	4.09	4.11
FBI employees who comprise the general workforce set a positive example for their peers and coworkers by adhering to applicable rules, regulations, and policies	4.16	4.22	4.10
I am reluctant to report incidents of non-compliance with applicable rules, regulations, and policies due to the possible consequences of reporting them	3.84	3.90	3.90
If I see someone else engaging in misconduct, I will report it to the appropriate authorities	4.07	4.06	4.09
FBI executive management has made clear that a commitment to ethics, integrity, and compliance is an institutional priority	4.08	4.12	4.20
I am able to identify and communicate key risks within my area of responsibility	Not asked	3.98	4.00
The importance of risk management and control has been communicated to me through specific training, supervisor communications, and policy and practice in my squad or unit.	Not asked	3.79	3.87
I understand the level of risk I can take on behalf of the FBI involving override or alteration of internal control procedures or policies	Not asked	3.66	3.73
I can easily find authoritative, usable policy information	3.31	3.32	3.06
Management is receptive to all communications about risk, including bad news	3.12	3.58	3.60
I believe FBI executive managers set a positive example for the organization by adhering to applicable rules, regulations, and policies	3.33	3.46	3.56

Note: Survey respondents answer each question depending on their level of agreement with the statement on a scale of 1 (strongly disagree) through 5 (strongly agree). However, some questions are worded negatively; therefore, they are re-coded so that the higher number is always better. The FBI then computed an average of responses to generate a score between 1 and 5.

Source: FBI employee survey.

APPENDIX VI: FBI RESPONSE TO DRAFT REPORT



U.S. Department of Justice

Federal Bureau of Investigation

Office of Integrity and Compliance

Washington, D.C. 20535

November 14, 2011

Cynthia A. Schnedar
Acting Inspector General
Office of the Inspector General
U.S. Department of Justice
Suite 4706
950 Pennsylvania Avenue, NW
Washington, D.C. 20530

Dear Ms. Schnedar:

The Federal Bureau of Investigation (FBI) appreciates the opportunity to review and respond to your draft report on "The Federal Bureau of Investigation's Integrity and Compliance Program [ICP]."

Compliance with the Constitution, individual and institutional integrity, and accountability are core values of the FBI. Further, it is our policy to comply fully with all laws and rules governing our operations and to adhere to the highest standards of ethical conduct. To better implement that policy and advance our Core Values, we established the ICP. We note that the report found the Office of Integrity and Compliance has "enhanced" the FBI's ethics program and "promotes" reporting of compliance concerns. We are also pleased that the report found that, "[t]hrough the ICP, the FBI implemented strategies that have started to reduce legal compliance risk in FBI operations." The report states that the ICP establishes a "systematic process for risk identification" and has improved FBI senior management's knowledge of, and response to, compliance risks. We agree with the report that the implementation of the ICP marked a "fundamental change" in how the FBI identifies and manages legal compliance risks before they develop into problems. We are proud to have taken this step towards good governance.

Enclosed herein are the FBI's responses to the report's recommendations. Please feel free to contact me at 202-324-6829 should you have any questions or need further information.

Sincerely,

Patrick W. Kelley
Assistant Director
Office of Integrity and Compliance

Enclosure

OIG Review of the FBI's Integrity and Compliance Program

Recommendation #1 - Increase awareness of the Compliance Helpline and other OIC human resource initiatives.

FBI Response to Recommendation #1:

The Office of Integrity and Compliance (OIC) concurs with this recommendation. In Fiscal Year (FY) 12, OIC intends to develop and implement a plan to increase awareness of the Compliance Helpline and other OIC human resource initiatives such as the Director's Compliance Award.

Recommendation #2 - Consider using a formal methodology that includes specific criteria that participants must consider when assessing and prioritizing risk.

FBI Response to Recommendation #2:

OIC concurs with this recommendation. When OIC was formed, a formal risk assessment methodology was developed as one of many tools to assist management in the identification of potential risks. OIC still uses this risk methodology tool and periodically trains leadership on its use to ensure Executive Management Committee (EMC) participants understand and consider this criteria when assessing and prioritizing risk. During this past round of EMC meetings in October and November of 2011, OIC provided training to each committee on the risk assessment methodology. These criteria were identified as one tool which should be considered in conjunction with a variety of other factors impacting the risk assessment and prioritization process. These other factors include staffing limitations (on either OIC or on the risk owner), resource limitations, and the risk owner's mission priorities. All of these factors should be taken into consideration when selecting a risk. Using the corporate compliance sector as a model, OIC believes that compliance is the business of each executive. Each FBI executive is uniquely positioned to understand and appreciate his or her risk areas and mission. Ultimately, OIC defers to the executive in the selection of a potential risk for analysis.

Recommendation #3 - Increase Assistant Director involvement in program-level risk mitigation.

FBI Response to Recommendation #3:

OIC concurs with this recommendation. Pursuant to FBI Corporate Policy Directive 0126D, all managers of major programs must submit their semi-annual compliance risk report "up to and including the Assistant Director level and OIC." Pursuant to this Directive, OIC will remind major program managers of this requirement in the coming year. During this most recent set of quarterly EMC meetings, OIC provided training to each committee, to include Assistant Directors. A component of this training addressed the reporting requirement for major program managers and reminded Assistant Directors of their role in the process.

Recommendation #4 - Require program-level risks to include a verification step.

FBI Response to Recommendation #4

OIC concurs with this recommendation. Staffing limitations, however, constrain OIC's ability to verify mitigation efforts for every risk reported by 53 major programs. In FY12, OIC will establish a random verification process for major programs and will require verification of mitigation efforts for a sampling of programs during each of the two reporting periods.

Recommendation #5 - Comply with existing requirements for an annual report assessing the effectiveness of the ICP; for example, a report that articulates the program's goals, shows progress towards accomplishing them, and identifies areas for improvement.

FBI Response to Recommendation #5:

OIC concurs with this recommendation. It bears noting that at present, OIC provides a monthly compliance update chart to every senior executive within the FBI. On a quarterly basis, each branch holds a meeting to discuss its compliance risks. OIC uses these meetings to provide training, update on risks and to articulate program initiatives. Three times per year, senior executives meet with the Director of the FBI to discuss compliance risks. Similar to the quarterly meetings, OIC uses this medium as a way to provide updates on OIC initiatives and risk analysis and mitigation efforts.

APPENDIX VII: OIG ANALYSIS OF FBI RESPONSE

The Office of the Inspector General provided a draft of this report to the Federal Bureau of Investigation for its comment. The report contained five recommendations for consideration. The FBI's response is included in Appendix VI to this report. The OIG's analysis of the FBI's response and the actions necessary to close the recommendations are discussed below.

Recommendation 1. Increase awareness of the Compliance Helpline and other OIC human resource initiatives.

Status. Resolved – open.

Summary of the FBI Response. The FBI concurred with the recommendation and stated that in fiscal year (FY) 2012, the OIC intends to develop and implement a plan to increase awareness of the Compliance Helpline and other OIC human resource initiatives such as the Director's Compliance Award.

OIG Analysis. The actions taken and planned by the FBI are responsive to our recommendation. By February 29, 2012, please provide the OIG with a plan that describes the specific actions the OIC will take to increase awareness of the Compliance Helpline and other OIC human resource initiatives, and the dates by which the OIC plans to complete those activities, or a status of your progress.

Recommendation 2. Consider using a formal methodology that includes specific criteria that participants must consider when assessing and prioritizing risk.

Status. Resolved – open.

Summary of the FBI Response. The FBI concurred with this recommendation and stated that “when the OIC was formed, a formal risk assessment methodology was developed as one of many tools to assist management in the identification of potential risks,” and that the OIC still uses this risk methodology tool. According to the FBI, the OIC provided training on the methodology to Executive Management Committee members during committee meetings in October and November 2011. The training presented the methodology as “one tool which should be considered in conjunction with a variety of other

factors” such as staffing limitations, resource limitations, and the risk owner’s mission priorities in assessing and prioritizing risk.

OIG Analysis. The actions taken by the FBI are responsive to our recommendation. By February 29, 2012, please provide the OIG documentation of the October and November 2011 training, including the training materials and a list of who attended.

Recommendation 3. Increase Assistant Director involvement in program-level risk mitigation.

Status. Resolved – open.

Summary of the FBI Response. The FBI concurred with this recommendation and noted that pursuant to FBI Corporate Policy Directive 0126D, “all managers of major programs must submit their semi-annual compliance risk report up to and including the Assistant Director level and OIC.” The FBI also stated that the OIC will remind major program managers of this requirement in the coming year. Further, the FBI stated that the most recent quarterly Executive Management Committee meetings included training that “addressed the reporting requirement of major program managers and reminded Assistant Directors of their role in the process.”

OIG Analysis. The FBI’s actions are responsive to our recommendation. However, we note that so far, submitting the program manager reports to the Assistant Directors has not resulted in sufficient Assistant Director involvement in program-level risk mitigation. By February 29, 2012, please provide documentation of the reminders of the reporting and participation requirements given to Assistant Directors, a description of the role Assistant Directors will have in program-level risk mitigation, and the specific actions the FBI will take to increase their involvement. Additionally, please provide documentation that all major programs required to participate in program-level risk mitigation did participate. If the OIC exempted any major programs, include the reason for the exemption.

Recommendation 4. Require program-level risks to include a verification step.

Status. Resolved – open.

Summary of the FBI Response. The FBI concurred with our recommendation and stated that in FY 2012, the OIC will establish “a

random verification process for major programs and will require verification of mitigation efforts for a sampling of programs during each of the two reporting periods.” The FBI added that because of staffing limitations, the OIC will not be able to verify mitigation efforts for every risk reported by 53 major programs in every cycle.

OIG Analysis. The FBI’s actions are responsive to this recommendation. By February 29, 2012, please provide a specific description of how the OIC will conduct its verification process to ensure that each program is sampled every 2 years. In addition, please provide the results of all the verifications that the OIC completes by February 2012.

Recommendation 5. Comply with existing requirements for an annual report assessing the effectiveness of the ICP, for example, a report that articulates the program’s goals, shows progress toward accomplishing them, and identifies areas for improvement.

Status. Resolved – open.

Summary of the FBI Response. The FBI concurred with our recommendation. The FBI also noted several existing processes for updating managers about current compliance efforts. These processes include the OIC providing a monthly compliance update chart to every senior executive within the FBI; the use of Executive Management Committee quarterly meetings for the OIC to provide training, update participants on risks, and articulate program initiatives; and that three times per year, senior executives meet with the Director of the FBI to discuss compliance risks.

OIG Analysis. Although the FBI concurred with our recommendation, its response did not describe how it would respond to the recommendation that it produce an annual report of the ICP’s effectiveness. We note that while the monthly updates and discussions during meetings that the FBI describes in its response are useful, they are not a replacement for an annual report that articulates the program’s goals, shows progress toward accomplishing them, and identifies challenges and areas for improvement. By February 29, 2012, please provide a description of the FBI’s plan for satisfying the recommendation that it produce an annual written report of the ICP’s activities and effectiveness.