

## **Foreword**

Pursuant to Section 521(c) of the Implementing Recommendations of the 9/11 Commission Act, the Chief Privacy and Civil Liberties Officer for the Department of Justice, the Civil Liberties Protection Officer of the Office of the Director of National Intelligence, and the Officer for Civil Rights and Civil Liberties for the U.S. Department of Homeland Security present the Civil Liberties Impact Assessment of the Interagency Threat Assessment and Coordination Group, which facilitates the sharing of national intelligence information with state, local, and tribal entities.

Pursuant to congressional requirements, this Impact Assessment is being provided to the following:

Secretary of Homeland Security

Director, Federal Bureau of Investigation

United States Attorney General

Director, National Counterterrorism Center

Director of National Intelligence

Privacy and Civil Liberties Oversight Board

Committee on Homeland Security and Governmental Affairs of the Senate

Committee on Homeland Security of the House of Representatives

Select Committee on Intelligence of the Senate

Permanent Select Committee on Intelligence of the House of Representatives



Civil Liberties Impact Assessment  
for the  
**Interagency Threat Assessment and  
Coordination Group (ITACG)**

September 29, 2010

**Reviewing Officials**

**Margo Schlanger**

Officer for Civil Rights and Civil Liberties  
U.S. Department of Homeland Security  
(202) 357-7765

**Alexander W. Joel**

Civil Liberties Protection Officer  
Office of the Director of National Intelligence  
(703) 275-3589

**Nancy C. Libin**

Chief Privacy and Civil Liberties Officer  
U.S. Department of Justice  
(202) 307-0697

**ITACG Contact Point**

Tamara Hutchinson, Director  
Interagency Threat Assessment and Coordination Group  
(571) 280-6201



## I. INTRODUCTION

The September 11, 2001 attacks spurred the United States to reexamine its defense, intelligence, and law enforcement priorities and structure. In its report issued July 2004, the Commission on Terrorist Attacks Upon the United States (“9/11 Commission”) highlighted the threat of international terrorist groups and identified gaps in information sharing capabilities as a contributing factor in the Government’s failure to prevent the attack.<sup>1</sup> The President established the Interagency Threat Assessment and Coordination Group (ITACG) to address some of these gaps,<sup>2</sup> and Congress subsequently codified the group’s existence, creating an ITACG Detail and an ITACG Advisory Council.<sup>3</sup> Both the Detail and the Council are led by senior federal law enforcement and intelligence personnel but consist primarily of representatives from State and local government. By statute, the Detail’s purpose is to improve the sharing of intelligence between the Intelligence Community<sup>4</sup> (IC) and State, local, and tribal (“State and local”) governments; the Council’s purpose is to oversee the Detail. Congress further directed the undersigned Officers to assess the civil liberties impact of the ITACG and to submit to Congress a report discussing our findings.<sup>5</sup> This Civil Liberties Impact Assessment meets that requirement.<sup>6</sup> The scope of this Impact Assessment is restricted to the activities of ITACG Detail; it does not address broader issues of terrorism information sharing between federal, State and local entities via the Information Sharing Environment (ISE).<sup>7</sup>

As detailed in the Facts section below, the ITACG improves information sharing between the IC and State and local governments primarily by recommending and facilitating the dissemination of national intelligence products that may be of use to State and local government officials. This

---

<sup>1</sup> *The Final Report of the National Commission on Terrorist Attacks Upon the United States* (“*The 9/11 Commission Report*”), §§ 3.4 & 13.2.

<sup>2</sup> Program Manager, Information Sharing Environment, *Report on the Interagency Threat Assessment Group 3* (2009).

<sup>3</sup> See section 521 of the *Implementing Recommendations of the 9-11 Commission Act of 2007*, 6 U.S.C. § 124k (2007).

<sup>4</sup> The “intelligence community” or IC is a group of 17 agencies and organizations within the executive branch that work both independently and collaboratively to gather the intelligence necessary to conduct foreign relations and national security activities. The IC includes the Department of Homeland Security Office of Intelligence & Analysis as well as the Office of the Director of National Intelligence, which houses the National Counterterrorism Center. For a complete listing of the agencies constituting the IC, please see section 3(4) of the *National Security Act of 1947*, codified at 50 U.S.C. § 401a(4), as well as section 3.5(h) of Executive Order 12333.

<sup>5</sup> See 6 U.S.C. § 124k(b)(2) (2007). Section 521(c) of the *Implementing Recommendations of the 9-11 Commission Act of 2007* requires the Department of Homeland Security Officer for Civil Rights and Civil Liberties and the Department of Justice Chief Privacy and Civil Liberties Officer, in consultation with the Civil Liberties Protection Officer of the Office of the Director of National Intelligence, to submit reports assessing the civil liberties impact of the ITACG.

<sup>6</sup> A Privacy Impact Assessment was prepared in July 2008, as also required by the statute.

<sup>7</sup> The ISE is an interrelated set of harmonized policies, mission processes, and systems leveraging common core capabilities to allow federal, State, and local entities to access and share terrorism information in a manner consistent with national security and with applicable legal and policy standards relating to privacy, civil rights, and civil liberties. See section 1016 of the *Intelligence Reform and Terrorism Prevention Act of 2004*, 6 U.S.C. § 485 (2007).



Impact Assessment assesses three ways by which ITACG activities could potentially affect individuals' rights. First, one or more Detail members might improperly rely on race, ethnicity, religion, or other suspect classifications to select a biased array of products for dissemination. Such decisions could cause State and local decision-makers, even those acting in good faith, to focus security measures on members of the groups improperly singled out. Second, a Detail member could improperly disseminate or disclose sensitive personal information, or inaccurate information relating to individuals mentioned in intelligence products, potentially causing serious and unwarranted harm to affected reputations, careers, or personal lives. Third, provision of intelligence information, which is frequently incomplete and inconclusive, to State and local entities unaccustomed to interpreting and using intelligence information could cause unintended and unproductive overreaction that undermines individual rights. These are real risks, and they warrant focused attention.

We conclude that existing training, supervision, and oversight of ITACG activities are sufficient to mitigate these risks. Nevertheless, we recommend that the ITACG Advisory Council include in its policies on the operation of the Detail, currently under development, guidance on information access and dissemination, as well as the use of race, ethnicity, religion, and other suspect classifications. Inclusion of these topics will provide Detail members additional clear, written guidance on inappropriate or unlawful dissemination or criteria for selection and recommendation of products, and reinforce the application of the National Counterterrorism Center's existing operational policies to ITACG operations.

To conduct this assessment, our offices relied on program documents (including, but not limited to, the memorandum of agreement on the establishment and operation of the ITACG and the draft ITACG standard operating procedures), interviews and briefings with National Counterterrorism Center (NCTC) and Department of Homeland Security Office of Intelligence & Analysis (DHS I&A) staff, consultation with the Federal Bureau of Investigation (FBI),<sup>8</sup> the authorizing legislation, congressional testimony, and outside reports. In addition, the DHS Office for Civil Rights and Civil Liberties (CRCL) participated in departmental planning for the ITACG, including providing input on various ITACG documents, testimony, briefings, and correspondence, as part of its regular statutory duties requiring CRCL to "oversee compliance with constitutional, statutory, regulatory, policy, and other requirements relating to the civil rights and civil liberties of individuals affected by the programs and activities of the Department."<sup>9</sup> In addition, in the course of researching and writing this impact assessment, CRCL consulted with the DHS Office of the General Counsel, whose legal views are incorporated throughout.

In short, the conclusions presented here are those of the undersigned Officers, but we have reached them after substantial consultation with the DHS Office of the General Counsel; DHS I&A; the Program Manager, Information Sharing Environment; legal counsel for the NCTC; the Detail's leadership; and the DOJ National Security Division. We thank them for their time,

---

<sup>8</sup> The Deputy Director of the ITACG is an FBI official and the FBI has assigned one intelligence analyst to the ITACG.

<sup>9</sup> 6 U.S.C. § 345(a)(4) (2004).



professionalism, and commitment to ensuring that the ITACG improves information sharing with State and local entities without diminishing anyone's civil rights or civil liberties.

## II. FACTS

The NCTC, an element of the ODNI, is the U.S. Government's central clearinghouse of information relating to terrorism (except for information pertaining exclusively to domestic terrorism), providing federal agencies with terrorism intelligence analysis products. The terrorism-related informational needs and interests of federal, State, and local governments are diverse. The federal focus is typically on problems of national and international scope and particular investigations. Although State and local governments participate in relevant investigations, their day-to-day focus is on local and regional counterterrorism and security issues, particularly on identifying and protecting critical infrastructure, and on developing detailed emergency preparedness and response plans. As a result, there is always a risk that State and local terrorism information needs may be overlooked within the IC, including at the NCTC. One of the 9/11 Commission's major recommendations was the improvement of information sharing.<sup>10</sup> The ITACG constitutes one of the President's and Congress's answers to that call.

The Detail operates within the NCTC chain of command and answers to the Director of NCTC or his designee. The ITACG Director, a senior DHS employee, manages the day-to-day operations of the Detail. The staff of the Detail includes State and local law enforcement officers and first responders detailed to DHS via an Intergovernmental Personnel Act agreement, and then assigned from DHS to work with counterterrorism analysts at NCTC. Currently, the Detail has funding for ten positions; there is no cap on how many individuals may serve on the Detail in either the authorizing legislation or memorandum of agreement that governs its operation. Assignments are generally limited to one-year rotations. For operational purposes, State and local Detail members are treated as federal employees and are subject to ODNI and DHS oversight and supervision.

The ITACG Detail complements and enhances the ISE by bringing State and local personnel into the IC, where they can work to identify federal information that may meet State and local terrorism information needs. The Detail performs three sets of tasks: (1) recommending the dissemination, and sometimes modification, of existing intelligence products; (2) advocating the needs of State and local governments for terrorism information; and (3) recommending and assisting in the production of a limited number of original intelligence products, in concert with IC partners. Each is discussed below.

First, the Detail identifies existing intelligence products produced by IC elements and recommends dissemination, sometimes after modification, of some of those products. Modifications the Detail might recommend could, for example, include changes to allow the lowering of the classification level and therefore broader dissemination among first responders, or the addition of context to make the information more useful to State and local decision-makers. If the originating agency concurs with the Detail's recommendations, it modifies the

---

<sup>10</sup> *The 9/11 Commission Report* at § 13.3.



product. Then, with originating agency consent, these products are forwarded to DHS, the Federal Bureau of Investigation (FBI), or other appropriate federal agencies, which may, at their discretion and using their existing information sharing infrastructure, disseminate the products to State and local entities. The Detail reviews hundreds of intelligence products each month. Typically, it recommends State and local dissemination of 5-10 of them; most of these recommendations include suggested modifications.

Second, the Detail advocates within the NCTC for State and local information needs related to terrorism. Members of the Detail focus on building relationships with the IC elements represented at the NCTC; the Detail's blend of federal, State, and local personnel allows it to provide useful advice and insight to those elements. The Detail also meets with State and local consumers of intelligence products to clarify State and local needs and elicit feedback on previously disseminated products.

Third, the Detail recommends the development of original intelligence products by the IC elements present at NCTC. For instance, the *Roll Call Release*—produced jointly by DHS and FBI, based in part on recommendations from the Detail—provides unclassified information for rank and file law enforcement personnel relating to terrorism trends, tactics, techniques, and procedures. The *Roll Call Release* was initiated in December 2008; as of September 30, 2010, 51 editions have been published.

The ITACG also occasionally produces technical assistance documents for State and local entities. For example, the *ITACG Intelligence Guide for First Responders* explains to State and local decision-makers how to interpret federal intelligence products, including how to weigh the credibility of sources and reliability of information. It also clearly states the standards for the safeguarding of data and penalties for failing to do so. Currently, the Detail plans an update to its *ITACG Intelligence Guide for First Responders*, and to produce a similar pocket guide for police officers focused on terrorism tactics, techniques, and procedures.

The ITACG Advisory Council oversees the Detail. It is chaired by the DHS Under Secretary for I&A, led by senior federal law enforcement and intelligence officials, and composed largely of senior State and local law enforcement and intelligence executives. Through the Council, the Under Secretary for I&A, on behalf of DHS and in coordination with the Director of NCTC, develops policies, procedures, guidance, and standards that help the Detail perform its mission. The Council's focus through 2009 was on drafting procedures to identify and recruit qualified State and local personnel to staff the Detail. Those procedures were developed after coordination with DHS, ODNI, and the Attorney General. The Council's focus has now shifted to improving the Detail's policies and procedures, and ultimately its effectiveness. By statute, the Council meets at least quarterly but in fact has been meeting more often—8 times in calendar-year 2009 and 5 times between January and September 2010—to fulfill operational needs.



### **III. ISSUES**

As noted above, Detail members do not themselves collect, retain, analyze, or disseminate information. This Impact Assessment accordingly does not assess the civil rights and civil liberties issues embedded in information collection, retention, analysis, or dissemination. It is relevant, however, that numerous oversight bodies periodically (and in some instances routinely) review intelligence products within the NCTC and at the agencies that are, in fact, responsible for disseminating the products. Specific items that raise civil rights or civil liberties concerns may be detected through the oversight by NCTC supervisory, legal, technical, and Executive Order 12333 (E.O. 12333) oversight offices, in consultation with the ODNI Civil Liberties and Privacy Office, or by comparable structures within the FBI, DOJ, and DHS. For example, within DHS, the I&A Intelligence Oversight Officer works with CRCL, the DHS Privacy Office, and the DHS Office of the General Counsel to review intelligence products prior to dissemination, ensuring compliance with applicable civil rights, civil liberties, privacy laws and policies, and requirements under E.O. 12333.

The ITACG Detail's roles in the intelligence life cycle, as elaborated above, are: to review thousands of intelligence products for possible relevance to State and local personnel, provide assistance in the modification and reissuance of hundreds of such products newly tailored to meet State and local needs, and make suggestions to the IC about needs for new products. These roles raise three potential civil rights and civil liberties issues. First, Detail members could improperly rely on race, ethnicity, religion, or other constitutionally suspect classifications in making decisions about which products to prioritize for dissemination to State and local officials. Second, Detail members could improperly disclose sensitive personal information or incorrect or embarrassing information relating to individuals mentioned in intelligence products, using contacts with their home agencies or informal networks rather than official channels. Such disclosures could, in turn, cause unwarranted damage to an individual's reputation, career, or personal life. Third, information sharing with State and local entities could induce overreactions by some users of terrorism-related intelligence; users who lack the necessary skill or context to properly interpret intelligence products may respond to tentative or partial information in a manner that is overbroad or overzealous, considering sources and uncertainties.

#### ***A. Race/Ethnicity/Religious Bias in Product Selection***

With reference to the potential for biased selection of products for State and local dissemination, we note that the ITACG's memorandum of agreement requires it to abide by all applicable federal laws, executive orders, directives, and other presidential guidance in the protection of the legal rights of Americans, which includes the right to be free from invidious discrimination on the basis of race, ethnicity, or religion. In order to meet this obligation, the ITACG Advisory Council requires Detail members to receive the same training as new NCTC employees, including legal compliance training. This training includes intelligence oversight, information handling, and privacy and civil liberties training provided by the NCTC Office of General Counsel. It specifically covers the IC oversight architecture, E.O. 12333, and the U.S. Person rules, which implement constitutional and other legal protections for individuals who are mentioned in intelligence products. In addition, new Detail members receive training from the



ODNI Civil Liberties and Privacy Office, including training on the prohibition against focusing programs or activities based solely on race, ethnicity, religion of the subjects or their First Amendment activities, as well as the Privacy Act, and E.O. 12333 and the U.S. Person rules. The training serves to reinforce to each member of the ITACG staff that race, ethnicity, or religion should not serve as the basis for any dissemination of intelligence products.

Currently, the ITACG Advisory Council is developing policy documents to memorialize existing standard procedures regarding the operation of the Detail, including defining the criteria that may be used in recommending products for dissemination, or in the creation of new products. Detail leadership reports that the Detail does not seek to identify particular individuals with known or suspected terrorist ties, or to search existing products by relying on demographic characteristics. They report that the Detail focuses instead on identifying products that provide information regarding terrorist tactics, techniques, and procedures. The Detail also actively seeks the feedback of State and locals on products and areas of concern through face-to-face meetings at conferences of State and local law enforcement and emergency response organizations. The Detail also receives feedback from the disseminating agencies, which interact with the State and local entities regularly.

Similarly, the Detail has strong operational incentives to rely on facts rather than racial or ethnic prejudice or other forms of improper stereotyping. As recent arrests involving al-Qa'ida supporters and other individuals alleged to have committed ideologically motivated violence demonstrate, the demographics of those who commit such acts do not necessarily conform to popular stereotypes. Because terrorists may be of any given race, ethnicity, gender, or nationality, and may adhere to any one of a number of belief systems, simple tradecraft provides a very strong motivation for Detail members to keep an open mind about where threats may originate, and to avoid making decisions based on grounds that are unrelated to actual threat information. Efforts by an individual Detail member to select products for dissemination, or to create new products, based on stereotypes or prejudice rather than facts would stand out and draw scrutiny. Because of the strong operational interest of Detail management, NCTC, FBI, and DHS, products fitting such a pattern would be questioned and the resulting products likely withheld from dissemination.

Finally, we note that in discussing the ITACG Detail's activities with Detail leadership, DHS and FBI overseers, fusion center personnel, and others who have contact with the Detail's work, we have received no complaints of racial, ethnic, or religious bias in product selection. And in reading about a hundred of the products that the Detail proposed for dissemination, our staffs detected no racial, ethnic, or religious tilt to the selections, compared to the underlying universe of intelligence products with which we are familiar. This comparison was informal; we did not conduct any statistical analysis, because we detected no need for such an undertaking.

### ***B. Improper Dissemination of Intelligence Information***

A second way the ITACG might conceivably undermine individual rights is if Detailees improperly used the federal systems to which the Detail grants them access. For example, Detail staff might improperly disseminate intelligence products to personnel at their home agency, and





improperly disclose sensitive personal information or incorrect or embarrassing information relating to individuals mentioned in those intelligence products. We believe the probability of this kind of abuse is low.

With respect to all intelligence information, the rules are clear: ITACG personnel are prohibited by law and NCTC policy from sharing any information obtained in the course of their duties through personal rather than official channels. This prohibition includes but is not limited to information about individuals or groups protected by the U.S. Constitution and other federal laws and policies, including both U.S. Persons<sup>11</sup> and non-resident aliens.

Information about U.S. Persons, in particular, is protected through E.O. 12333 and applicable implementing guidelines. Intelligence oversight is grounded in E.O. 12333, and the NCTC has its own set of guidelines implementing that Executive Order's rules, including among other things, U.S. Person rules and procedures for reporting potential violations. E.O. 12333 and its implementing guidelines permit NCTC to acquire U.S. Person information only to determine if the information constitutes terrorism information as defined in Section 1016 of the Intelligence Reform and Terrorism Prevention Act and thus, properly may be retained, used and disseminated.<sup>12</sup> The ITACG is governed by these same rules. There is, moreover, a presumption that unless determined otherwise, all individuals currently within the United States are U.S. Persons. Furthermore, the prohibition within E.O. 12333 against the violation of any federal law requires that the rights guaranteed to non-resident aliens will not be diminished by the activities of the IC.

The U.S. Person rules include a set of supervisory structures and procedures. Any ITACG activities believed to be unlawful or contrary to E.O. 12333 and falling within the criteria established by the Attorney General must be immediately reported by anyone with knowledge of a potential violation to the Intelligence Oversight Board of the President's Intelligence Advisory Board, the Director of National Intelligence, and, as appropriate, to Congress. Executive Order 13462 and the implementing guidance issued by the National Security Council further requires that "significant or highly sensitive matters, whether or not unlawful or contrary to Executive Order or presidential directive," be reported to the ODNI.

Detail products and IC products disseminated in coordination with the Detail are also subject to independent intelligence oversight at DHS and the FBI, which have parallel guidelines implementing E.O. 12333 and other applicable authorities. Thus, there is a high likelihood that reportable activities would be detected by an IC element handling Detail products and reported to the appropriate oversight authority. Additionally, the federal agencies providing personnel to serve at the Detail retain certain oversight authorities. The ODNI oversight authorities and the oversight and disciplinary authorities retained by "home" agencies serve together as a significant

---

<sup>11</sup> Per E.O. 12333 § 3.5(k), U.S. Persons means "a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments."

<sup>12</sup> See E.O. 12333 § 2.3 for a complete listing of the categories of U.S. Person information that may be collected.



deterrent and safeguard against Detailee misconduct at ITACG, just as they do elsewhere in the IC.

In particular, oversight specifically focused on civil rights and civil liberties is provided by the ODNI's Civil Liberties Protection Officer, who is charged with ensuring "compliance by the Office and the Director of National Intelligence with requirements under the Constitution and all laws, regulations, Executive orders, and implementing guidelines relating to civil liberties and privacy."<sup>13</sup> The ODNI Civil Liberties Protection Officer works closely with the NCTC, DHS, DOJ, and other IC agency legal counsel, as appropriate, to ensure all intelligence programs, including ITACG, adhere to these civil liberties and privacy requirements. Similar privacy, civil rights, and civil liberties oversight bodies operate within DHS, the FBI, and DOJ.

Members of the ITACG Detail are trained by the NCTC counsel's office on their responsibilities under E.O. 12333 and other "rules of the road" regarding access to and sharing of information. As part of the employee on-boarding process, they receive a full day of training that includes a briefing on applicable legal, policy, and procedural standards for the dissemination of products and the use of federal information systems; that training includes warnings about the penalties for misuse of the systems and for unauthorized disclosure of classified and sensitive information. New Detail members are specifically warned that disseminating information via personal, rather than official channels will result in official sanctions, up to and including dismissal from the NCTC. They are advised to seek release only through official channels if they identify a product that would be of interest to their home agencies. In addition, the DHS Privacy Office has instituted annual training on informational privacy issues, including limitations on sharing of personally identifiable information and warnings regarding the criminal and civil penalties for misuse of such information.

Moreover, the systems used by Detail personnel are subject to supervisory oversight and security monitoring. Detailees are notified of this fact in their initial briefings, and they are reminded each time they log on to a national security system, with some warnings including a discussion of possible penalties. Security and supervisory oversight includes monitoring of all computer activities, including access to intelligence, security and other databases and information systems, email, and Internet activity, allowing the Government to detect and trace misuse to particular operators. Release of a product by an individual Detail member via the NCTC computer system would be easily traceable; while relay of information by phone or smuggling of documents out of the facility is less traceable, computer system access monitoring is available to assist in identifying violators who disclose information by other means. As authorized dissemination of IC products to State and local entities occurs through—and at the sole discretion of—DHS and the FBI, any dissemination of an IC product to a State or local entity by an individual Detail member would be unquestionably outside of official channels.

Detail leadership believes the combination of notices, monitoring, and strong sanctions for violations is a significant disincentive to the potential misuse or abuse of national security information. Detail leadership explains that Detailees are aware that a violation would result in

---

<sup>13</sup> National Security Act of 1947, as amended, at § 103D(b)(2), 50 U.S.C. § 403-3d(b)(2) (2005).



dismissal for cause from the Detail, and that this would likely cause severe professional repercussions upon a Detailee's return to the home agency. And again, in the course of the extended period of time in which this Impact Assessment has been underway, we are not aware of even one account of a Detail member disclosing information relating to individuals mentioned in intelligence products through unofficial channels. If an individual believes that his or her information has been misused, existing statutes provide for complaint evaluation by the DHS Inspector General, the DHS Chief Privacy Officer, the DHS Officer for Civil Rights and Civil Liberties, the ODNI Civil Liberties Protection Officer, and the DOJ Office of the Inspector General—contact information is included on the last page of this Impact Assessment. No such complaints have been received to date.

### ***C. Encouragement of Overreaction, or Overbroad Reaction***

A third potential problem is inherent in information sharing with State and local law enforcement, because State and local personnel tend to be less familiar with context, uncertainties, and terminology involved in interpreting and using federal terrorism-related intelligence than most of the more traditional (and frequent) users. Federal intelligence products not tailored to meet State and local needs may thereby create a serious problem for the decision-makers who rely on them. The products may raise the specter of a grave terrorist threat but then fail to provide sufficient contextual information about the threat posed, or may not provide information that helps the decision-maker evaluate the credibility of the source and reliability of the information. State and local decision-makers may then feel compelled to take action but lack sufficient information to develop a response that is appropriate to the threat. During our review, we heard repeatedly from State and local law enforcement leaders that they and their peers need sufficient information, placed in proper context, to help them avoid overreactions that could infringe on individual rights.

Again, this is a serious concern, with two possible responses. The first is to not share information with State and local entities. But Congress has determined (quite appropriately in our view) that the benefits of sharing outweigh the risks—and has eliminated this option by codifying the ITACG. The second response to the risk posed by acontextual information-sharing is to share information in a way that *does* provide context and guidance regarding the credibility of the threat, so that State and local partners can take an informed course of action, responding to what is known about the threat in a tailored, appropriate manner—in other words, to do what the Detail does.

The very purpose of the ITACG Detail is to promote provision of actionable, appropriately tailored intelligence to State and local decision-makers to meet their needs. A good example of how the Detail addresses existing limitations in information sharing is contained in the *ITACG Intelligence Guide for First Responders*, which is a manual instructing State and local personnel on how to interpret federal IC products. The *Guide* includes instruction on giving intelligence products proper weight in decision-making, based in part on the credibility of intelligence sources relied upon, and the degree to which the source information has been confirmed. This framework for understanding how to read intelligence products helps decision-makers at all levels respond appropriately to threats and avoid overreactions that could erroneously impair



individual rights. To our knowledge, this is the first time a concerted national effort has been made to educate State and local decision-makers on how to understand intelligence products. In short, the problem identified is real, and it is a structural problem inherent in information sharing—but the ITACG ameliorates rather than exacerbates this problem.

#### **IV. RECOMMENDATIONS**

The ITACG focuses on identifying and recommending the production and dissemination of products that provide information on terrorist tactics, training and procedures, rather than on individual terrorists, and those recommendations are subject to multiple layers of oversight by the originating and disseminating agencies, which determine the final content of any product and whether it will be disseminated, as well as oversight by the ODNI's Civil Liberties Protection Officer. Therefore, we determine that the risk is low that Detail members would improperly rely on race, ethnicity, religion, or other constitutionally suspect classifications to select products for recommended dissemination. The training that Detail members receive, coupled with the operational incentives to rely on facts rather than prejudice or stereotypes, further reduce this risk. Nevertheless, we recommend that the ITACG Advisory Council include guidance on the use of race, ethnicity, religion, and other constitutionally suspect classifications in its policies on the operation of the Detail, which are currently under development. The undersigned Officers will assist the ITACG, NCTC and DHS I&A to evaluate the proposed policies and procedures. Policy on these topics would provide Detail members with further clear, written guidance on inappropriate or unlawful criteria for selection and recommendation of products. Similarly, although training, oversight, and monitoring significantly ameliorate the risk that Detail members will improperly disseminate intelligence information, we recommend the Advisory Council include reference to the NCTC policies on information access and dissemination in its policies regarding the operation of the Detail.

The undersigned Officers will continue to exercise their oversight authority to ensure that privacy, civil rights, and civil liberties are appropriately addressed in ITACG Detail activities, particularly in response to allegations of misconduct, abuse, or impropriety relating to individual rights.



Approval Signature Page

(Original signed and on file with the DHS Office for Civil Rights and Civil Liberties)

Office for Civil Rights and Civil Liberties

Margo Schlanger

Officer for Civil Rights and Civil Liberties

U.S. Department of Homeland Security

Office of the Director of National Intelligence

Alexander W. Joel

Civil Liberties Protection Officer

Office of the Director of National Intelligence

Office of the Deputy Attorney General

Nancy C. Libin

Chief Privacy and Civil Liberties Officer

U.S. Department of Justice



## **HOW TO FILE A COMPLAINT WITH DHS, DOJ, OR ODNI**

Information on the DHS civil rights and civil liberties complaint process, established by Section 705 of the Homeland Security Act of 2002, 6 U.S.C. § 345, and Section 1062 of the Intelligence Reform and Terrorism Prevention Act of 2004, 42 U.S.C. § 2000ee-1, is available at <http://www.dhs.gov/crcl>. An individual or group may file a civil rights or civil liberties complaint with the DHS Office for Civil Rights and Civil Liberties by e-mailing a complaint to [crcl@dhs.gov](mailto:crcl@dhs.gov) or mailing a complaint to the following address:

U.S. Department of Homeland Security  
Office for Civil Rights and Civil Liberties, Review and Compliance Unit  
Mail Stop #0190  
Washington, DC 20528

Information on the DHS Privacy complaint process, established by Section 222 of the Homeland Security Act of 2002, 6 U.S.C. § 142, is available at <http://www.dhs.gov/privacy>. An individual or group may file a privacy complaint with the DHS Chief Privacy Officer by e-mailing a complaint to [privacy@dhs.gov](mailto:privacy@dhs.gov) or mailing a complaint to the following address:

U.S. Department of Homeland Security  
Chief Privacy Officer  
Washington, DC 20528

Information on the DHS Office of the Inspector General complaint process, established by Section 8304 of the Intelligence Reform and Terrorism Prevention Act of 2004, 5 U.S.C. App.3 § 8I, is available at <http://www.dhs.gov/xoig>. An individual or group may file a complaint with the DHS Inspector General by emailing a complaint to [DHSOIGHOTLINE@dhs.gov](mailto:DHSOIGHOTLINE@dhs.gov) or mailing a complaint to the following address:

U.S. Department of Homeland Security  
Attn: Office of Inspector General, Hotline  
Washington, DC 20528

Pursuant to Section 103D of the National Security Act of 1947, 50 U.S.C. § 403-3d, an individual or group may file a complaint with the ODNI Civil Liberties Protection Officer by mailing a complaint to the following address:

Civil Liberties and Privacy Officer  
Office of the Director of National Intelligence  
Washington, DC 20511

Information on the DOJ Office of the Inspector General civil rights and civil liberties complaint process, established by Section 1001 of the USA Patriot Act, 5 U.S.C. App.3 § 8E, is available at <http://www.justice.gov/oig/FOIA/hotline2.htm>. An individual or group may file a complaint



with the DOJ Office of the Inspector General by emailing a complaint to [inspector.general@usdoj.gov](mailto:inspector.general@usdoj.gov) or mailing a complaint to the following address:

Civil Rights & Civil Liberties Complaints  
Office of the Inspector General  
U.S. Department of Justice  
950 Pennsylvania Avenue, N.W.  
Room 4706  
Washington, DC 20530