



governmentattic.org

"Rummaging in the government's attic"

Description of document: Seven (7) Treasury Inspector General for Tax Administration (TIGTA) Deputy Inspector General for Investigations (DIGI) memoranda, 2010-2017

Requested date: 31-March-2017

Released date: 01-May-2017

Posted date: 19-February-2018

Source of document: Office of Chief Counsel Disclosure Branch
Treasury Inspector General for Tax Administration
City Center Building
1401 H Street, NW, Suite 469
Washington, DC 20005
Fax: (202) 622-3339
Email: FOIA.Reading.Room@tigta.treas.gov

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

May 1, 2017

This is in response to your March 31, 2017 Freedom of Information Act (FOIA) request, seeking access to records maintained by the Treasury Inspector General for Tax Administration (TIGTA). The TIGTA Disclosure Branch received your e-mailed request on March 31, 2017.

Specifically, you requested a copy of the following Deputy Inspector General for Investigations (DIGI) Memoranda:

DIGI Memorandum 10-003, Access Granted to Previously Prohibited Websites.

DIGI Memorandum 11-007, Interim Guidance for the Potentially Dangerous Taxpayer Five Year Update Program.

DIGI Memorandum 12-004, Identify Theft Investigative Initiative.

DIGI Memorandum 15-005, Updated Department of Justice Guidance Regarding Use of Race and Other Characteristics by Federal Law Enforcement Agencies.

DIGI Memorandum 16-005, Body Worn Camera Program.

DIGI Memorandum 17-003, Updated Interim Guidance on the Body Worn Camera Program.

DIGI Memorandum 17-002, Criminal Results Management System (CRIMES) Interim Guidance.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S.C. § 552(c) (2006 & Supp. IV 2010). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

We have located thirty-nine (39) pages which are responsive to your request seeking copies of the above referenced Deputy Inspector General for Investigations (DIGI) Numbered Memoranda. We are releasing twenty-four (24) pages in full and six (6) pages in part. A copy is enclosed. We are withholding nine (9) pages in full. We are asserting FOIA subsections (b)(5), (b)(6), (b)(7)(C) and (b)(7)(E) as the justification for withholding.

FOIA subsection (b)(5) permits an agency to withhold inter-agency or intra-agency information that is considered to be part of the deliberative process. The type of information for which we assert the deliberative process under subsection (b)(5) consists of draft memoranda which contain opinions or recommendations which are predecisional in nature. Internal agency documents containing opinions, deliberations and recommendations of Agency employees in connection with their official duties are protected from disclosure pursuant to FOIA subsection (b)(5) and the deliberative process privilege.

FOIA subsection (b)(6) permits the withholding of records and information about individuals when disclosure of the information could result in a clearly unwarranted invasion of personal privacy. The withheld information consists of identifying information compiled with regard to individuals other than you. Releasing the withheld information would not shed any light into the Agency's performance of its official functions, but instead could result in an invasion into the personal privacy of the individuals whose names and personal information have been withheld. As a result, the privacy interests of the third parties outweigh the public's interest in having the information released.

FOIA subsection (b)(7)(C) permits an agency to withhold "information compiled for law enforcement purposes the release of which could reasonably be expected to constitute an unwarranted invasion of personal privacy." The withheld information consists of identifying information compiled with regard to individuals other than you. Releasing the withheld information would not shed any light into the Agency's performance of its official functions, but instead could result in an invasion into the personal privacy of the individuals whose names and personal information have been withheld. The information was compiled for law enforcement purposes and the privacy interest of the

third parties outweighs the public's interest in having the information released. As a result, this information has been withheld in response to your request.

FOIA subsection (b)(7)(E) permits an agency to withhold "records or information compiled for law enforcement purposes ... [that] would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." The withheld information consists of techniques or guidelines not commonly known to the public and/or information that could lead to the circumvention of the law. As a result, this information has been withheld in response to your request.

We have enclosed an Information Sheet that explains the subsections cited above as well as your administrative appeal rights. If you file an appeal, your appeal must be in writing, signed by you, and postmarked or electronically transmitted within ninety (90) days from the date of this letter. You should address the envelope as follows:

Freedom of Information Act Appeal
Treasury Inspector General for Tax Administration
Office of Chief Counsel
City Center Building
1401 H Street, NW, Suite 469
Washington, DC 20005

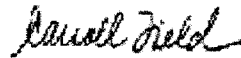
The cost incurred to process your FOIA request was less than \$25.00, the threshold set by Treasury's FOIA regulation, so no fees were assessed.

If you have any questions, please contact Carroll Field, Government Information Specialist, at (202) 927-7032 or Carroll.Field@tigta.treas.gov and refer to Disclosure File # 2017-FOI-00153.

You may contact our FOIA Public Liaison at (202) 622-4068 for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, MD

20740-6001; e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

Sincerely,

A handwritten signature in cursive script, appearing to read "Carroll Field".

Carroll Field

(For) Amy P. Jones
Disclosure Officer and
FOIA Public Liaison

Enclosures




INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

May 14, 2010

DIGI: 10-003

MEMORANDUM FOR ALL OFFICE OF INVESTIGATIONS EMPLOYEES

FROM: Steven M. Jones 
Deputy Inspector General for Investigations

SUBJECT: Access granted to previously prohibited websites

As discussed in DIGI Numbered Memorandum 10-001, the Office of Investigations (OI) strategic plan is focused on enhancing our abilities to develop investigations in the electronic environment. Recent Continuing Professional Education (CPE) cycles have been predominantly devoted to training in support of this goal. As you know, our goal is for all of you to become more conversant and proficient in the automated environment in order to further enhance our investigations and to free up our specialized expertise within the Strategic Enforcement Division (SED) to search for evolving criminal activities and new vulnerabilities which may adversely impact the integrity of Federal tax administration.

During the internet investigations block of the 2009 CPE cycle, we received a great deal of feedback from special agents who told us that they were unable to follow up on basic investigative leads because a number of common, popular websites were blocked by TIGTA's Office of Information Technology (OIT). Although frustrating, there were a number of valid reasons many sites were blocked including the concern over TIGTA's network security as mandated by the Federal Information Security Management Act (FISMA). FISMA requires the highest levels of accountability and oversight over Federal networks and it also requires that OIT annually certify that TIGTA's network is secure.

As promised during the discussions we had at the CPE sessions, we engaged OIT about obtaining access to previously restricted sites. I'm pleased to report we have achieved a compromise between ensuring network security and FISMA compliance and the need for OI special agents and investigative support personnel to have all the tools

required to conduct investigations in the electronic environment. As a result, access to the most potentially useful sites that were identified during the CPE has been provided to OI personnel (see below list). These sites will remain blocked to all other TIGTA functional entities. Part of the compromise with OIT is the understanding that, due to the increased security risk factors, these sites are to be accessed by OI employees for official investigative reasons only. In order to achieve our mutual goals, we are updating policy to reflect that access to these sites will be in relation to official investigative purposes. As with all investigative leads conducted, at a minimum you will be required to complete an entry on the respective Form 6501, Chronological Case Worksheet, to account for the access to any of the above listed websites. The entry on the Form 6501 will enable OI to account for the access if questioned.

Any misuse of the access to the sites will be dealt with accordingly as it raises not only the risk to the security of TIGTA's network, but also endangers the status of OI's enhanced, unrestricted access. I have assured OIT that OI personnel will conduct themselves in a professional manner, and that abuses will not occur.

Effective immediately, OI special agents and investigative support personnel have been granted access to the following sites:

www.youtube.com
www.facebook.com
www.myspace.com
www.ebay.com
www.classmates.com
www.craigslist.com
www.twitter.com
www.gunbroker.com

It is the steadfast goal of the OI executive team to provide you the best equipment, training and tools with which to perform your duties. To that end, I am very pleased that we were able to negotiate this favorable resolution. If, during your investigative efforts, you find that additional web-sites should rightly be added to this list, please have your Special Agent in Charge (SAC) contact the SAC-SED.



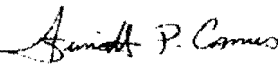
DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

July 27, 2011

TIGTA #11-07

MEMORANDUM FOR ALL OFFICE OF INVESTIGATIONS EMPLOYEES

FROM: Timothy P. Camus 
Deputy Inspector General for Investigations

SUBJECT: Interim Guidance for the Potentially Dangerous Taxpayer Five Year Update Program

Earlier this year, as a result of a study conducted in the aftermath of the attack on the Austin IRS office last February, the Office of Investigations (OI) assumed the expanded responsibility of receiving all armed escort requests from the IRS. This increased role has provided OI additional opportunities to show that we place a priority on our oversight of employee safety and physical security.

In addition to the armed escort issue, it was also determined that IRS employees were possibly exposed to a threatening environment as there was no systemic follow up investigation of all Potentially Dangerous Taxpayers (PDT) after their initial five year PDT designation expired. After much discussion and coordination with the Special Agents in Charge about this issue, it was decided that beginning August 1, 2011, OI will coordinate with the IRS Office of Employee Protection (OEP) to review PDT designations that are approaching their five year expiration date. OEP will continue to administer the PDT and Caution Upon Contact (CAU) programs; however OI will assume the responsibility for conducting the five year PDT update investigations. This additional responsibility will provide OI the opportunity to ensure that OEP has the information needed to effectively make their PDT extension determinations.

The OEP will provide OI a list of PDTs 90 days prior to their respective five year expiration date. Once received and triaged, OI will initiate an investigation, conduct criminal history research and make contact with local law enforcement for any information that may be available concerning the subject. OI will complete the

2

investigations within the 90 day period and forward the final report to OEP in order for them to determine if an extension is warranted.

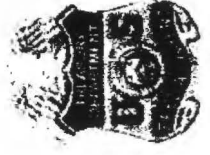
This interim guidance will serve as our policy until the Special Agent Handbook is updated in the near future. Please review the attached PowerPoint presentation for additional information. Any questions should be routed through your management team to Randy Silvis, Deputy Assistant Inspector General for Field Operations, at telephone number (b) (6) (b) (7)(C)



PDT 5 year
Presentation.pptx

Treasury Inspector General for Tax Administration (TIGTA)

Potentially Dangerous Taxpayer
(PDT) Five-Year Update Program



PDT Five-Year Update Program

- **Beginning August 1, 2011, the Office of Investigations (OI) will coordinate with the Internal Revenue Service (IRS) Office of Employee Protection (OEP) to evaluate PDT designations that are within 90 days of their five year expiration date.**



Electronic Crimes and Intelligence Division (ECID) responsibilities

- **CEP will send the PDT information to ECID.**
- **Within 10 days, ECID will initiate a complaint in PARIS.**
- **Complaints are transferred to the respective field divisions.**



Investigative Division responsibilities

- **Initiate investigation and at a minimum conduct the following investigative steps:**
- **Conduct criminal history research**
- **Contact appropriate law enforcement agencies to verify and obtain any additional information available related to the subject. This will include Federal, State, and Local law enforcement agencies.**



Investigative Division responsibilities

- **Refer to ECID for Intelligence Analyst Report (IAR) if appropriate.**
- **Refer Report of Investigation (ROI) to OEP before the PDT expiration date.**
- **All investigative steps should be recorded on Form 8501-
Chronological Case Worksheet (CCW).**



ROI

The ROI will be forwarded to IRS OEP; however, unlike the typical assault or threat investigation, the ROI will not need the following:

- Form 8273
- Subject interview
- A prosecutive opinion from the United State's Attorney's Office or State/Local prosecutor's office.





INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

April 16, 2012

DIGI 12-004

MEMORANDUM FOR ALL OFFICE OF INVESTIGATIONS EMPLOYEES

FROM:

Timothy P. Camus

A handwritten signature in black ink, appearing to read "Timothy P. Camus".

Deputy Inspector General for Investigations

SUBJECT:

Identity Theft Investigative Initiative

As you know, for the past several months IRS-related identity theft has been a hot issue. It has been widely covered in the media and it is of interest to the Congress. Recent identity theft schemes involve individuals or groups stealing identities and then filing fraudulent tax returns *before* the legitimate taxpayer files their own return. This results in refunds being issued to the criminals. On its surface, this crime is simple tax fraud and it is clearly within the jurisdiction of the IRS CI. However, there are other variations of IRS-related identity theft that fall within our jurisdiction.

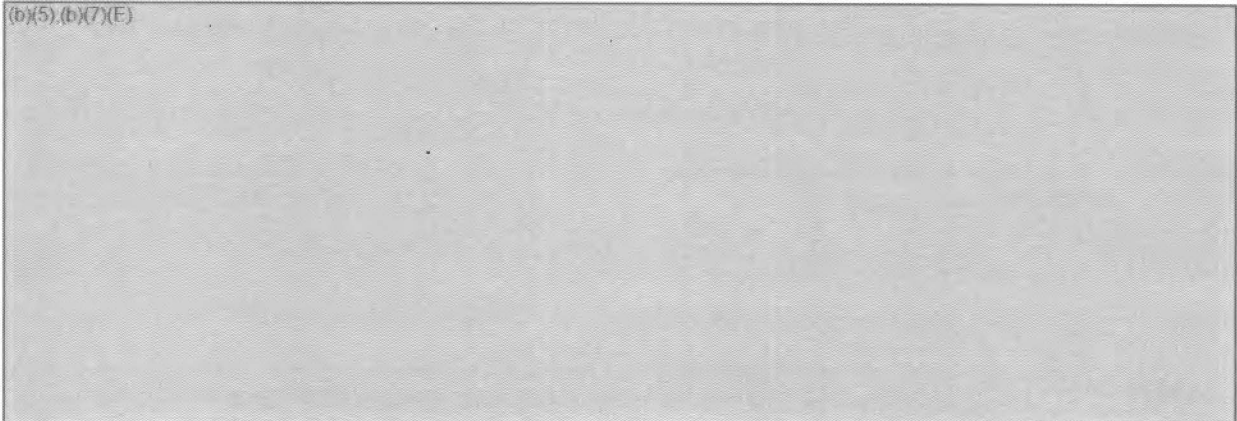
Our jurisdiction for identity theft purposes includes the following three areas:

- IRS employee involvement in the scheme - either through UNAX, disclosure or as a participant in the criminal activity;
- Preparers who misuse and disclose client information *to others* in furtherance of identity theft (excluding tax preparers who simply prepare and file fraudulent tax returns for the purpose of personally stealing the refund); and
- Impersonation of the IRS in furtherance of the identity theft scheme.

Recently we met with IRS leaders and other Federal and state law enforcement officials to determine the fact patterns relative to current identity theft schemes. After recent discussions with IRS leadership, we determined it is possible that the IRS-related identity theft schemes are being facilitated by individuals who have a strong working knowledge of IRS operations and or have access to IRS information. This added nuance poses an elevated risk to the integrity of IRS operations, and subsequently

invites a more aggressive approach from us to identify and combat IRS-related identity theft within our jurisdiction.

(b)(5), (b)(7)(E)



To ensure that OI remains engaged with other agencies' identity theft initiatives, we are appointing Senior Special Agent (b)(6), (b)(7)(C) as the program coordinator to establish national liaison with headquarters-based Federal law enforcement partners and to report to OI senior leaders on national and international identity theft trends and fact patterns as they become known. Special Agent (b)(6), (b)(7)(C) will also be responsible for reporting emerging identity theft trend information to the Field Divisions to assist in their investigations in this area.

(b)(6), (b)(7)(C)

(b)(5), (b)(7)(E)



As the DIGI, I balance the demands of our limited resources, ensuring that we maintain proper focus on our jurisdiction and that our investigative product is of the highest quality. The challenge is to balance our expanded investigative activity into identity theft against the need for resources to do our every day mission - realizing we will not receive additional funds from the Congress to do our job. Although not a perfect solution, I believe this is the best way to identify this type of criminal activity that falls within our jurisdiction, while maintaining the proper focus of our precious and limited resources.

Additional discussion and guidance will be forthcoming from your leadership team.



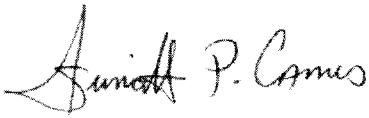
INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

March 5, 2015

DIGI: 15-005

MEMORANDUM FOR ALL SPECIAL AGENTS

FROM: Timothy P. Camus 
Deputy Inspector General for Investigations

SUBJECT: Updated Department of Justice Guidance Regarding Use of
Race and Other Characteristics by Federal Law Enforcement
Agencies

In December 2014, the Department of Justice (DOJ) updated its 2003 guidance on the use of race by law enforcement agencies. The 2014 Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity applies to Federal law enforcement officers performing Federal law enforcement activities, including those related to national security and intelligence, and defines not only the circumstances in which Federal law enforcement officers may take into account a person's race and ethnicity—as the 2003 guidance did—but also when gender, national origin, religion, sexual orientation, or gender identity may be taken into account.

The guidance sets out requirements beyond the Constitutional minimum that shall apply to the use of race, ethnicity, gender, national origin, religion, sexual orientation, and gender identity by Federal law enforcement officers. The guidance applies to such officers at all times, including when they are operating in partnership with non-Federal law enforcement agencies.

DOJ requires all law enforcement agencies to administer training on the guidance to all agents on a regular basis, including at the beginning of each agent's tenure. To comply with this requirement, OI is developing training regarding the new guidance which will be delivered to you through CPEs and/or the OI Training Academy.

The December 2014 guidance supersedes DOJ's 2003 *Guidance Regarding the Use of Race by Federal Law Enforcement Agencies*. This memorandum serves as interim guidance until Operations Manual Chapter 400, Section 20 is updated to reflect the new

guidance from DOJ. Please direct any questions regarding this guidance to the Special Agent in Charge, Operations Division, or to [*TIGTAInvOperations@tigta.treas.gov](mailto:TIGTAInvOperations@tigta.treas.gov).

U.S. Department of Justice

**GUIDANCE FOR FEDERAL LAW
ENFORCEMENT AGENCIES REGARDING
THE USE OF RACE, ETHNICITY, GENDER,
NATIONAL ORIGIN, RELIGION, SEXUAL
ORIENTATION, OR GENDER IDENTITY**



December 2014

INTRODUCTION AND EXECUTIVE SUMMARY

This Guidance supersedes the Department of Justice's 2003 Guidance Regarding the Use of Race by Federal Law Enforcement Agencies. It builds upon and expands the framework of the 2003 Guidance, and it reaffirms the Federal government's deep commitment to ensuring that its law enforcement agencies conduct their activities in an unbiased manner. Biased practices, as the Federal government has long recognized, are unfair, promote mistrust of law enforcement, and perpetuate negative and harmful stereotypes. Moreover—and vitally important—biased practices are ineffective. As Attorney General Eric Holder has stated, such practices are “simply not good law enforcement.”

Law enforcement practices free from inappropriate considerations, by contrast, strengthen trust in law enforcement agencies and foster collaborative efforts between law enforcement and communities to fight crime and keep the Nation safe. In other words, fair law enforcement practices are smart and effective law enforcement practices.

Even-handed law enforcement is therefore central to the integrity, legitimacy, and efficacy of all Federal law enforcement activities. The highest standards can—and should—be met across all such activities. Doing so will not hinder—and, indeed, will bolster—the performance of Federal law enforcement agencies' core responsibilities.

This new Guidance applies to Federal law enforcement officers performing Federal law enforcement activities, including those related to national security and intelligence, and defines not only the circumstances in which Federal law enforcement officers may take into account a person's race and ethnicity—as the 2003 Guidance did—but also when gender, national origin, religion, sexual orientation, or gender identity may be taken into account. This new Guidance also applies to state and local law enforcement officers while participating in Federal law enforcement task forces. Finally, this Guidance promotes training and accountability, to ensure that its contents are understood and implemented appropriately.

Biased law enforcement practices, as the 2003 Guidance recognized with regard to racial profiling, have a terrible cost, not only for individuals but also for the Nation as a whole. This new Guidance reflects the Federal government's ongoing commitment to keeping the Nation safe while upholding our dedication to the ideal of equal justice under the law.

Two standards in combination should guide use by Federal law enforcement officers of race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity in law enforcement or intelligence activities:

- In making routine or spontaneous law enforcement decisions, such as ordinary traffic stops, Federal law enforcement officers may not use race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity to any degree, except that officers may rely on the listed characteristics in a specific suspect description. This prohibition applies even where the use of a listed characteristic might otherwise be lawful.

- In conducting all activities other than routine or spontaneous law enforcement activities, Federal law enforcement officers may consider race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity only to the extent that there is trustworthy information, relevant to the locality or time frame, that links persons possessing a particular listed characteristic to an identified criminal incident, scheme, or organization, a threat to national or homeland security, a violation of Federal immigration law, or an authorized intelligence activity. In order to rely on a listed characteristic, law enforcement officers must also reasonably believe that the law enforcement, security, or intelligence activity to be undertaken is merited under the totality of the circumstances, such as any temporal exigency and the nature of any potential harm to be averted. This standard applies even where the use of a listed characteristic might otherwise be lawful.

DISCUSSION

The Constitution protects individuals against the invidious use of irrelevant individual characteristics. See *Whren v. United States*, 517 U.S. 806, 813 (1996). Such characteristics should never be the sole basis for a law enforcement action. This Guidance sets out requirements beyond the Constitutional minimum that shall apply to the use of race, ethnicity, gender, national origin,¹ religion, sexual orientation, and gender identity by Federal law enforcement officers.² This Guidance applies to such officers at all times, including when they are operating in partnership with non-Federal law enforcement agencies.

I. GUIDANCE FOR FEDERAL LAW ENFORCEMENT OFFICERS

A. Routine or Spontaneous Activities in Domestic Law Enforcement

In making routine or spontaneous law enforcement decisions, such as ordinary traffic stops, Federal law enforcement officers may not use race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity to any degree, except that officers may rely on the listed characteristics in a specific suspect description. This prohibition applies even where the use of a listed characteristic might otherwise be lawful.

¹ As used in this Guidance, “national origin” refers to an individual’s, or his or her ancestor’s, country of birth or origin, or an individual’s possession of the physical, cultural or linguistic characteristics commonly associated with a particular country. It does not refer to an individual’s “nationality” (i.e., country of citizenship or country of which the person is deemed a national), which may be relevant to the administration and enforcement of certain statutes, regulations, and executive orders.

² This Guidance is intended only to improve the internal management of the executive branch. It is not intended to, and does not, create any right, benefit, trust, or responsibility, whether substantive or procedural, enforceable at law or equity by a party against the United States, its departments, agencies, instrumentalities, entities, officers, employees, or agents, or any person, nor does it create any right of review in an administrative, judicial, or any other proceeding. This Guidance does not apply to Federal non-law enforcement personnel, including U.S. military, intelligence, or diplomatic personnel, and their activities. In addition, this Guidance does not apply to interdiction activities in the vicinity of the border, or to protective, inspection, or screening activities. All such activities must be conducted consistent with the Constitution and applicable Federal law and policy, in a manner that respects privacy, civil rights and civil liberties, and subject to appropriate oversight.

Law enforcement agencies and officers sometimes engage in law enforcement activities, such as traffic and foot patrols, that generally do not involve either the ongoing investigation of specific criminal activities or the prevention of catastrophic events or harm to national or homeland security. Rather, their activities are typified by spontaneous action in response to the activities of individuals whom they happen to encounter in the course of their patrols and about whom they have no information other than their observations. These general enforcement responsibilities should be carried out without *any* consideration of race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity.

- **Example:** While parked by the side of the George Washington Parkway, a Park Police Officer notices that nearly all vehicles on the road are exceeding the posted speed limit. Although each such vehicle is committing an infraction that would legally justify a stop, the officer may not use a listed characteristic as a factor in deciding which motorists to pull over. Likewise, the officer may not use a listed characteristic in deciding which detained motorists to ask to consent to a search of their vehicles.

Some have argued that overall discrepancies in certain crime rates among certain groups could justify using a listed characteristic as a factor in general traffic enforcement activities and would produce a greater number of arrests for non-traffic offenses (*e.g.*, narcotics trafficking). We emphatically reject this view. Profiling by law enforcement based on a listed characteristic is morally wrong and inconsistent with our core values and principles of fairness and justice. Even if there were overall statistical evidence of differential rates of commission of certain offenses among individuals possessing particular characteristics, the affirmative use of such generalized notions by law enforcement officers in routine, spontaneous law enforcement activities is tantamount to stereotyping. It casts a pall of suspicion over every member of certain groups without regard to the specific circumstances of a particular law enforcement activity, and it offends the dignity of the individual improperly targeted. Whatever the motivation, it is patently unacceptable and thus prohibited under this Guidance for law enforcement officers to act on the belief that possession of a listed characteristic signals a higher risk of criminality. This is the core of invidious profiling, and it must not occur.

The situation is different when an officer has specific information, based on trustworthy sources, to “be on the lookout” for specific individuals identified at least in part by a specific listed characteristic. In such circumstances, the officer is not acting based on a generalized assumption about individuals possessing certain characteristics; rather, the officer is helping locate specific individuals previously identified as involved in crime.

- **Example:** While parked by the side of the George Washington Parkway, a Park Police Officer receives an “All Points Bulletin” to be on the lookout for a fleeing bank robbery suspect, a man of a particular race and particular hair color in his 30s driving a blue automobile. The officer may use this description, including the race and gender of the particular suspect, in deciding which speeding motorists to pull over.

B. All Activities Other Than Routine or Spontaneous Law Enforcement Activities

In conducting all activities other than routine or spontaneous law enforcement activities, Federal law enforcement officers may consider race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity only to the extent that there is trustworthy information, relevant to the locality or time frame, that links persons possessing a particular listed characteristic to an identified criminal incident, scheme, or organization, a threat to national or homeland security, a violation of Federal immigration law, or an authorized intelligence activity. In order to rely on a listed characteristic, law enforcement officers must also reasonably believe that the law enforcement, security, or intelligence activity to be undertaken is merited under the totality of the circumstances, such as any temporal exigency and the nature of any potential harm to be averted. This standard applies even where the use of a listed characteristic might otherwise be lawful.³

As noted above, there are circumstances in which law enforcement officers engaged in activities relating to particular identified criminal incidents, schemes, organizations, threats to national or homeland security, violations of Federal immigration law, or authorized intelligence activities may consider personal identifying characteristics of potential suspects, including race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity. Common sense dictates that when a victim describes the assailant as possessing a certain characteristic, law enforcement officers may properly limit their search for suspects to persons possessing that characteristic. Similarly, in conducting activities directed at a specific criminal organization or terrorist group whose membership has been identified as overwhelmingly possessing a listed characteristic, law enforcement should not be expected to disregard such facts in taking investigative or preventive steps aimed at the organization's activities.

Reliance upon generalized stereotypes involving the listed characteristics is absolutely forbidden. In order for law enforcement officers to rely on information about a listed characteristic, the following must be true:

- The information must be relevant to the locality or time frame of the criminal activity, threat to national or homeland security, violation of Federal immigration law, or authorized intelligence activity;
- The information must be trustworthy; and
- The information concerning identifying listed characteristics must be tied to a particular criminal incident, a particular criminal scheme, a particular criminal organization, a threat to national or homeland security, a violation of Federal immigration law, or an authorized intelligence activity.

³ This Guidance does not prohibit the accommodation of religious beliefs and practices consistent with the U.S. Constitution and federal law. The Guidance also does not prohibit officials from considering gender when "the gender classification is not invidious, but rather realistically reflects the fact that the sexes are not similarly situated." *Rostker v. Goldberg*, 453 U.S. 57, 79 (1981).

Because law enforcement and intelligence actions are necessarily context-specific, in applying each of these factors, law enforcement officers may properly account for relevant facts and circumstances, such as any temporal exigency and the nature of any potential harm to be averted. However, in all cases, law enforcement officers must reasonably believe that the law enforcement or intelligence activity to be undertaken is merited under the totality of the circumstances.

The following policy statements more fully explain these principles.

1. *Law Enforcement Officers May Never Rely on Generalized Stereotypes, But May Rely Only on Specific Characteristic-Based Information*

This standard categorically bars the use of generalized assumptions based on listed characteristics.

- **Example:** In the course of investigating an auto theft ring in a Federal park, law enforcement officers could not properly choose to target individuals of a particular national origin as suspects, based on a generalized assumption that those individuals are more likely to commit crimes.

This bar extends to the use of pretexts as an excuse to target minorities. Officers may not use such pretexts. This prohibition extends to the use of other, facially neutral factors as a proxy for overtly targeting persons because of a listed characteristic. This concern arises most frequently when aggressive law enforcement efforts are focused on “high crime areas.” The issue is ultimately one of motivation and evidence; certain seemingly characteristic-based efforts, if properly supported by reliable, empirical data, are in fact neutral.

- **Example:** In connection with a new initiative to increase drug arrests, law enforcement officers begin aggressively enforcing speeding, traffic, and other public area laws in a neighborhood predominantly occupied by people of a single race. The choice of neighborhood was not based on the number of 911 calls, number of arrests, or other pertinent reporting data specific to that area, but only on the general assumption that more drug-related crime occurs in that neighborhood because of its racial composition. This effort would be improper because it is based on generalized stereotypes.
- **Example:** Law enforcement officers seeking to increase drug arrests use tracking software to plot out where, if anywhere, drug arrests are concentrated in a particular city, and discover that the clear majority of drug arrests occur in particular precincts that happen to be neighborhoods predominantly occupied by people of a single race. So long as they are not motivated by racial animus, officers can properly decide to enforce all laws aggressively in that area, including less serious quality of life ordinances, as a means of increasing drug-related arrests. *See, e.g., United States v Montero-Camargo*, 208 F.3d 1122, 1138 (9th Cir. 2000) (“We must be particularly careful to ensure that a ‘high crime’ area factor is not used with respect to entire neighborhoods or communities in which members of minority groups regularly go

about their daily business, but is limited to specific, circumscribed locations where particular crimes occur with unusual regularity.”).

By contrast, where law enforcement officers are investigating a crime and have received *specific information* that the suspect possesses a certain listed characteristic (e.g., direct observations by the victim or other witnesses), the officers may reasonably use that information, even if it is the only descriptive information available. In such an instance, it is the victim or other witness making the classification, and officers may use reliable incident-specific identifying information to apprehend criminal suspects. Officers, however, must use caution in the rare instance in which a suspect’s possession of a listed characteristic is the only available information. Although the use of that information may not be unconstitutional, broad targeting of discrete groups always raises serious fairness concerns.

- **Example:** The victim of an assault describes her assailant as an older male of a particular race with a birthmark on his face. The investigation focuses on whether any men in the surrounding area fit the victim’s description. Here investigators are properly relying on a description given by the victim, which included the assailant’s race and gender, along with his age and identifying personal characteristic. Although the ensuing investigation affects individuals of a particular race and gender, that investigation is not undertaken with a discriminatory purpose. Thus use of race and gender as factors in the investigation, in this instance, is permissible.

2. The Information Must be Relevant to the Locality or Time Frame

Any information that law enforcement officers rely upon concerning a listed characteristic possessed by persons who may be linked to specific criminal activities, a threat to national or homeland security, a violation of Federal immigration law, or an authorized intelligence activity must be locally or temporally relevant.

- **Example:** Five years ago, DEA issued an intelligence report that indicated that a drug ring whose members are known to be predominantly of a particular ethnicity is trafficking drugs in Charleston, SC. An agent operating in Los Angeles reads this intelligence report. In the absence of information establishing that this intelligence is also applicable in Southern California or at the present time, the agent may not use ethnicity as a factor in making local law enforcement decisions about individuals who are of the particular ethnicity that was predominant in the Charleston drug ring.

3. The Information Must be Trustworthy

Where the information relied upon by law enforcement officers linking a person possessing a listed characteristic to potential criminal activity, a threat to national or homeland security, a violation of Federal immigration law, or an authorized intelligence activity is unreliable or is too generalized and unspecific, reliance on that characteristic is prohibited.

- **Example:** ATF special agents receive an uncorroborated anonymous tip that a male of a particular ethnicity will purchase an illegal firearm at a Greyhound bus terminal

in an ethnically diverse North Philadelphia neighborhood. Although agents surveilling the location are free to monitor the movements of whomever they choose, the agents are prohibited from using the tip information, without more, to target any males of that ethnicity in the bus terminal. *Cf. Morgan v. Woessner*, 997 F.2d 1244, 1254 (9th Cir. 1993) (finding no reasonable basis for suspicion where tip “made all black men suspect”). The information is neither sufficiently reliable nor sufficiently specific.

In determining whether information is trustworthy, an officer should consider the totality of the circumstances, such as the reliability of the source, the specificity of the information, and the context in which it is being used.

- **Example:** ICE receives an uncorroborated anonymous tip indicating that females from a specific Eastern European country have been smuggled into Colorado and are working at bars in a certain town. Agents identify a group of women wearing t-shirts with the logo of a local bar who seem to be speaking an Eastern European language. The agents approach the group to ask them questions about their immigration status. Because the women match the specific information provided by the tipster, the information is sufficient under the circumstances to justify the agents’ actions.

4. *Characteristic-Based Information Must Always be Specific to Particular Suspects or Incidents; Ongoing Criminal Activities, Schemes, or Enterprises; a Threat to National or Homeland Security; a Violation of Federal Immigration Law, or an Authorized Intelligence Activity*

These standards contemplate the appropriate use of both “suspect-specific” and “incident-specific” information. As noted above, where a crime has occurred and law enforcement officers have eyewitness accounts including the race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity of the perpetrator, that information may be used. Law enforcement officers may also use reliable, locally or temporally relevant information linking persons possessing a listed characteristic to a particular incident, unlawful scheme, or ongoing criminal enterprise, a threat to national or homeland security, a violation of Federal immigration law, or an authorized intelligence activity—even absent a description of any particular individual suspect. In certain cases, the circumstances surrounding an incident, ongoing criminal activity, threat to national or homeland security, or violation of Federal immigration law will point strongly to a perpetrator possessing a specific listed characteristic, even though law enforcement officers lack an eyewitness account.

- **Example:** The FBI is investigating the murder of a known gang member and has information that the shooter is a member of a rival gang. The FBI knows that the members of the rival gang are exclusively members of a certain ethnicity. This information, however, is not suspect-specific because there is no description of the particular assailant. But because law enforcement officers have reliable, locally or temporally relevant information linking a rival group with a distinctive ethnic character to the murder, the FBI could properly consider ethnicity in conjunction with other appropriate factors in the course of conducting their investigation. Agents

could properly decide to focus on persons dressed in a manner consistent with gang activity, but ignore persons dressed in that manner who do not appear to be members of that particular ethnicity.

- **Example:** Local law enforcement arrests an individual, and in the course of custodial interrogation the individual states that he was born in a foreign country and provides other information that reasonably leads local law enforcement to question his immigration status. Criminal background checks performed by the local law enforcement agency reveal that the individual was recently released from state prison after completing a lengthy sentence for aggravated sexual assault. Local law enforcement contacts ICE to inquire as to the individual's immigration status. When ICE's database check on the immigration status of the arrestee does not locate a record of the individual's lawful immigration status, ICE sends an officer to the jail to question the individual about his immigration status, whereupon the individual states that he entered the United States without authorization and has never regularized his status. ICE assumes custody of the individual and processes him for removal from the United States. ICE properly relied on the facts presented to it, including that the arrestee was born in a foreign country, in searching its immigration database and conducting its subsequent investigation.

In addition, law enforcement officers may use a listed characteristic in connection with source recruitment, where such characteristic bears on the potential source's placement and access to information relevant to an identified criminal incident, scheme, or organization, a threat to national or homeland security, a violation of Federal immigration law, or an authorized intelligence activity.

- **Example:** A terrorist organization that is made up of members of a particular ethnicity sets off a bomb in a foreign country. There is no specific information that the organization is currently a threat to the United States. To gain intelligence on the evolving threat posed by the organization, and to gain insight into its intentions regarding the U.S. homeland and U.S. interests, the FBI may properly consider ethnicity when developing sources with information that could assist the FBI in mitigating any potential threat from the organization.

5. Reasonably Merited Under the Totality of the Circumstances

Finally, when a law enforcement officer relies on a listed characteristic in undertaking an action, that officer must have a reasonable belief that the action is merited under the totality of the circumstances. This standard ensures that, under the circumstances, the officer is acting in good faith when he or she relies in part on a listed characteristic to take action.

- **Example:** A law enforcement officer who is working as part of a federal task force has received a reliable tip that an individual intends to detonate a homemade bomb in a train station during rush hour, but the tip does not provide any more information. The officer harbors stereotypical views about religion and therefore decides that investigators should focus on individuals of a particular faith. Doing so would be

impermissible because a law enforcement officer's stereotypical beliefs never provide a reasonable basis to undertake a law enforcement or intelligence action.

Note that these standards allow the use of reliable identifying information about planned future crimes, attacks, or other violations of Federal law. Where officers receive a credible tip from a reliable informant regarding a planned crime or attack that has not yet occurred, the officers may use this information under the same restrictions applying to information obtained regarding a past incident. A prohibition on the use of reliable prospective information would severely hamper law enforcement efforts by essentially compelling law enforcement officers to wait for incidents to occur, instead of taking pro-active measures to prevent them from happening.

- **Example:** While investigating a specific drug trafficking operation, DEA special agents learn that a particular methamphetamine distribution ring is manufacturing the drug in California, and plans to have couriers pick up shipments at the Sacramento, California, airport and drive the drugs back to Oklahoma for distribution. The agents also receive trustworthy information that the distribution ring has specifically chosen to hire older women of a particular race to act as the couriers. DEA agents may properly target older women of that particular race driving vehicles with indicia such as Oklahoma plates near the Sacramento airport.

6. National and Homeland Security and Intelligence Activities

Since the terrorist attacks on September 11, 2001, Federal law enforcement agencies have used every legitimate tool to prevent future attacks and deter those who would cause devastating harm to our Nation and its people through the use of biological or chemical weapons, other weapons of mass destruction, suicide hijackings, or any other means. "It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." *Haig v. Agee*, 453 U.S. 280, 307 (1981) (quoting *Aptheker v. Secretary of State*, 378 U.S. 500, 509 (1964)).

The years since September 11 have also demonstrated that Federal law enforcement officers can achieve this critical goal without compromising our cherished value of equal justice under the law. Every day, Federal law enforcement officers work to keep our Nation safe, and they do so without invidious profiling. The standard embodied in this Guidance thus applies to Federal law enforcement agencies' national and homeland security operations, which will continue to focus on protecting the public while upholding our values.

National security, homeland security, and intelligence activities often are national in scope and focused on prevention of attacks by both known and unknown actors, not just prosecution. For example, terrorist organizations might aim to engage in acts of catastrophic violence in any part of the country (indeed, in multiple places simultaneously, if possible). These facts do not change the applicability of the Guidance, however. In order to undertake an action based on a listed characteristic, a law enforcement officer must have trustworthy information, relevant to the locality or time frame, linking persons possessing that characteristic

to a threat to national security, homeland security, or intelligence activity, and the actions to be taken must be reasonable under the totality of the circumstances.

- **Example:** The FBI receives reliable information that persons affiliated with a foreign ethnic insurgent group intend to use suicide bombers to assassinate that country's president and his entire entourage during an official visit to the United States. Agents may appropriately focus investigative attention on identifying members of that ethnic insurgent group who may be present and active in the United States and who, based on other available information, might be involved in planning some such attack during the state visit.
- **Example:** A citizen of Country A, who was born in Country B, lawfully entered the United States on an F-1 student visa. The school that the individual was supposed to attend notifies ICE that he failed to register or attend the school once in the United States, in violation of the terms of his visa. ICE has intelligence that links individuals with ties to Country B who have registered at that school to a designated terrorist organization that has made statements about launching an attack against the United States. ICE selects the individual for investigation, identification, location, and arrest. Once taken into custody, the individual is questioned and a decision is made to place him in removal proceedings and to detain him during those proceedings. ICE's decision to prioritize this immigration status violator for investigation and arrest was proper because it was based upon a combination of the factors known about the individual, including his national origin, school affiliation, and behavior upon arrival in the United States.

Good law enforcement work also requires that officers take steps to know their surroundings even before there is a specific threat to national security. Getting to know a community and its features can be critical to building partnerships and facilitating dialogues, which can be good for communities and law enforcement alike. Law enforcement officers may not, however, target only those persons or communities possessing a specific listed characteristic without satisfying the requirements of this Guidance.

- **Example:** An FBI field office attempts to map out the features of the city within its area of responsibility in order to gain a better understanding of potential liaison contacts and outreach opportunities. In doing so, the office acquires information from public sources regarding population demographics, including concentrations of ethnic groups. This activity is permissible if it is undertaken pursuant to an authorized intelligence or investigative purpose. The activity would not be permitted without such an authorized purpose or in circumstances that do not otherwise meet the requirements of this Guidance.

ADDITIONAL REQUIREMENTS

In order to ensure its implementation, this Guidance finally requires that Federal law enforcement agencies take the following steps on training, data collection, and accountability.

Training

Training provides agents and officers with an opportunity to dedicate their attention to a task, to learn about the factual application of theoretical concepts, and to learn from their colleagues. Training also provides an opportunity to ensure that consistent practices are applied across the agency.

Law enforcement agencies therefore must administer training on this Guidance to all agents on a regular basis, including at the beginning of each agent's tenure. Training should address both the legal authorities that govern this area and the application of this Guidance. Training will be reviewed and cleared by agency leadership to ensure consistency through the agency.

Data Collection

Data collection can be a tremendously powerful tool to help managers assess the relative success or failure of policies and practices. At the same time, data collection is only useful to the extent that the collected data can be analyzed effectively and that conclusions can be drawn with confidence.

Each law enforcement agency therefore (i) will begin tracking complaints made based on the Guidance, and (ii) will study the implementation of this Guidance through targeted, data-driven research projects.

Accountability

Accountability is essential to the integrity of Federal law enforcement agencies and their relationship with the citizens and communities they are sworn to protect. Therefore, all allegations of violations of this Guidance will be treated just like other allegations of misconduct and referred to the appropriate Department office that handles such allegations. Moreover, all violations will be brought to the attention of the head of the Department of which the law enforcement agency is a component.



INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

September 29, 2016

DIGI 16-005

MEMORANDUM FOR ALL OFFICE OF INVESTIGATIONS EMPLOYEES

FROM:

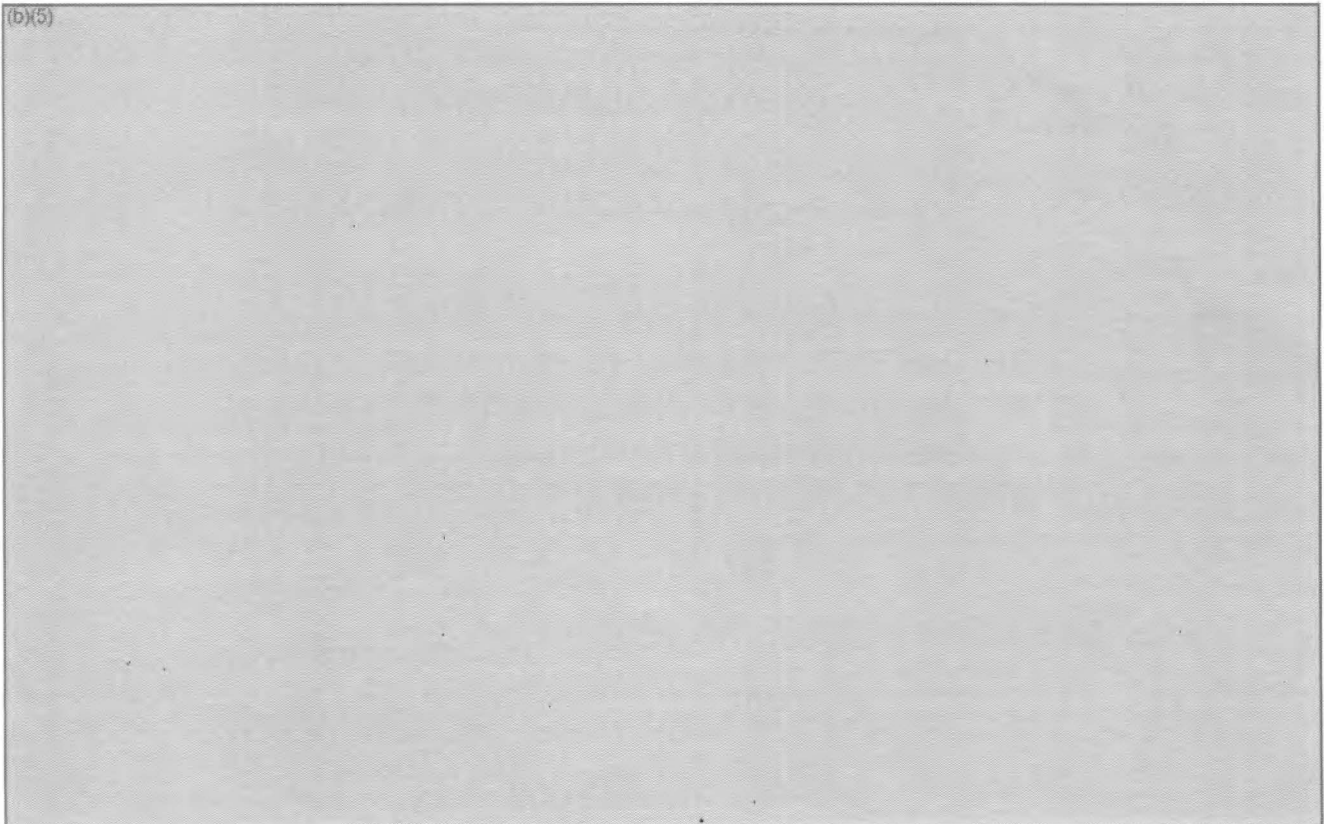
Timothy P. Camus 
Deputy Inspector General for Investigations

SUBJECT:

Body Worn Camera Program

As members of the law enforcement community, we are constantly reminded of the inherent risks and increasing dangers that we face while conducting our official activities. We in the Office of Investigations (OI) are committed to ensuring that all OI special agents are properly equipped and trained to conduct law enforcement activities in a safe and effective manner.

(b)(5)





INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

October 31, 2016

DIGI 17-003

MEMORANDUM FOR ALL OFFICE OF INVESTIGATIONS EMPLOYEES

FROM:

Timothy P. Camus

Deputy Inspector General for Investigations

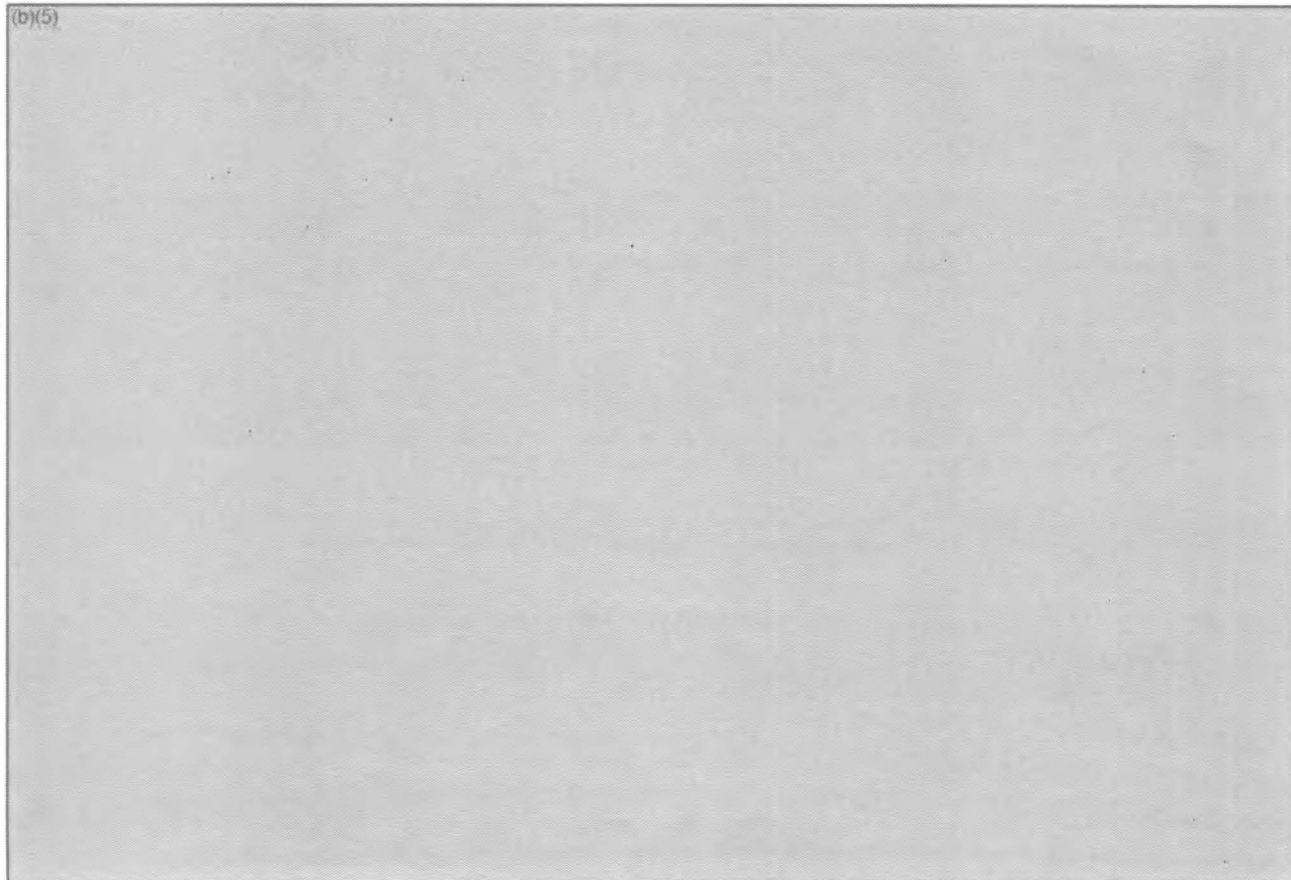
A handwritten signature in black ink, appearing to read "Timothy P. Camus".

SUBJECT:

Updated Interim Guidance on the Body Worn Camera Program

This memorandum serves as the Office of Investigations (OI) updated interim guidance related to the Body Worn Camera (BWC) Program.

(b)(5)





INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

October 28, 2016

DIGI: 17-002

MEMORANDUM FOR ALL OFFICE OF INVESTIGATION EMPLOYEES

FROM:

Timothy P. Camus 
Deputy Inspector General for Investigations

SUBJECT: Criminal Results Management System (CRIMES) Interim Guidance

This document serves as the Office of Investigations (OI) interim guidance related to the November 1, 2016, rollout of OI's new records management system, the Criminal Results Management System (CRIMES), which replaces the Performance and Results Information System (PARIS).

As outlined in the October 12, 2016, Program Guidance Document for Fiscal Year 2017, OI has successfully completed the development of CRIMES. For the last couple of years, OI has been in need of a replacement case management system for PARIS that would allow for future growth and provide upgraded analytics and report generating capability. CRIMES will enhance the efficiency of OI's workflow, provide us with new statistical and analytical tools, allow for better case management for our staff, as well as enable us to more effectively track and report on our vital statistics.

The CRIMES project team has worked tirelessly to bring us the most comprehensive and inclusive records management system possible for use in our daily investigative activities. The project team members, along with the divisional CRIMES training representatives, have spent the last several months providing personalized training to OI staff in order to give users an overview of the entire CRIMES system, as well as an opportunity for specialized hands-on instruction of the system's capabilities and features.

Once CRIMES is activated, a detailed *CRIMES User Guide* will be available in the system via the Help button, under *Guides and FAQs*. This user guide will be a fluid product with easy to follow instructions on how to create and input Contacts, Intakes (formerly Complaints), Cases, Initiatives, Time, and Acting or other Assignments, as well as descriptions of navigation terminology.

2

In order to ensure that the information contained in CRIMES is valid, it is imperative that all data is entered in an accurate, complete, and timely manner.

We are currently in the process of updating our policy (Chapter 400, Section 80) to reflect the implementation of CRIMES in place of PARIS. Until we formalize our new policy, OI staff will follow the procedures set forth in the *CRIMES User Guide*. Effective November 1, 2016, all Treasury Inspector General for Tax Administration Operations Manual references to PARIS should be recognized as equally applying to CRIMES, when applicable.

The CRIMES records system provides OI staff with access to large amounts of sensitive and protected information. Therefore, you are reminded that access to CRIMES and the records contained within it, is limited to official business only.

I want to acknowledge the dedication and commitment of the CRIMES project team, which includes Team Leader [REDACTED] ASAC [REDACTED] SA [REDACTED] Senior IT Specialists Chris Orcutt and Thomas Salter, and from TIGTA Information Technology (IT), Assistant Director Jerry Kim and IT Specialists Sunghee Heil, and Tomas Delgado. The project team has worked extremely hard in order to make CRIMES a reality. I want to recognize and thank each of them for their exceptional contributions to OI.