Report No. DODIG-2016-018

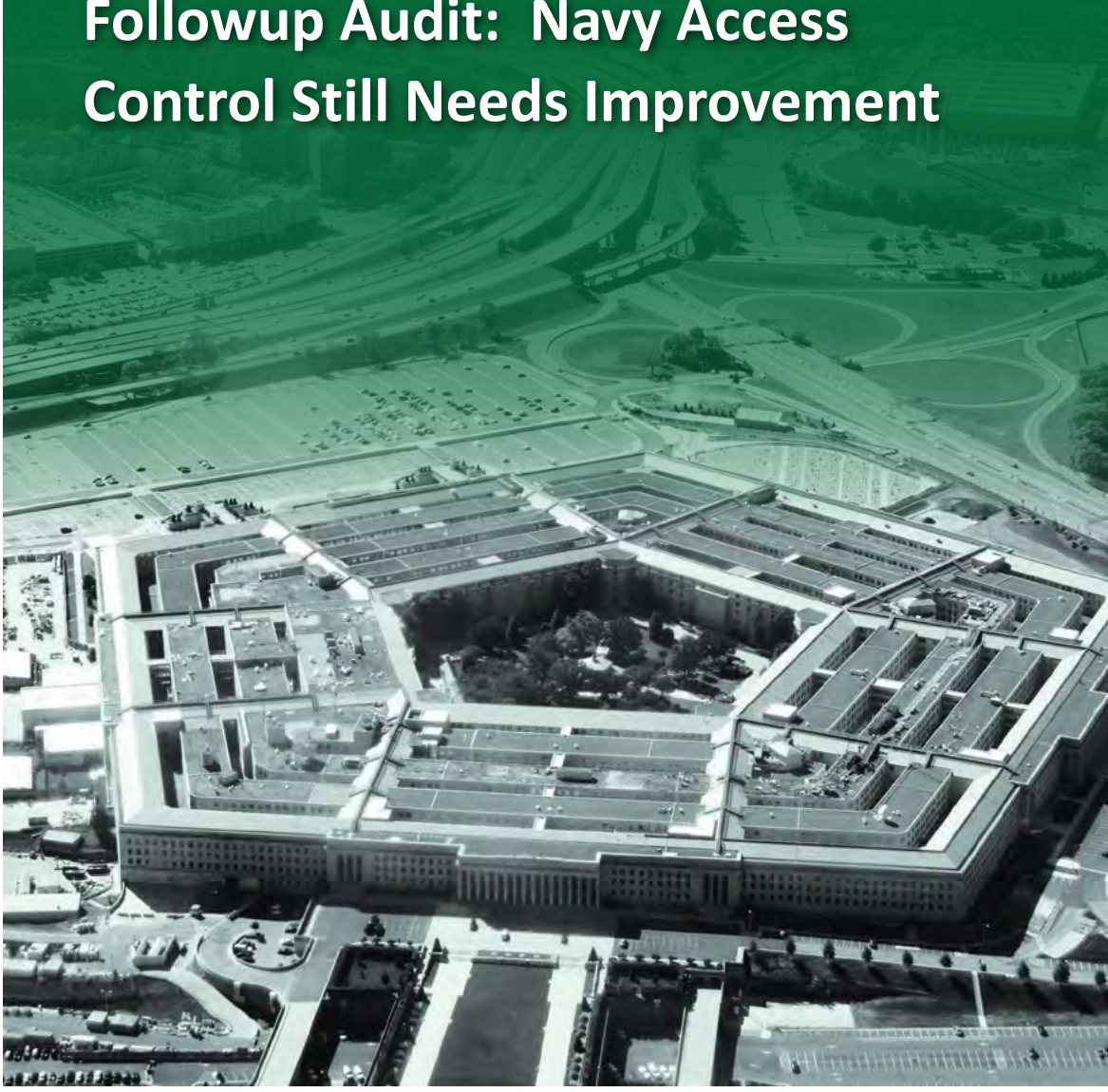
~~FOR OFFICIAL USE ONLY~~

# INSPECTOR GENERAL

*U.S. Department of Defense*

NOVEMBER 9, 2015

# Followup Audit: Navy Access Control Still Needs Improvement



INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

**The document contains information that may be exempt from mandatory disclosure under the Freedom of Information Act.**

~~FOR OFFICIAL USE ONLY~~

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

## Mission

*Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.*

## Vision

*Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.*


For more information about whistleblower protection, please see the inside back cover.

# Results in Brief

## *Followup Audit: Navy Access Control Still Needs Improvement*

**November 9, 2015**

## Objective

We determined whether the identified Navy installations implemented the agreed upon corrective actions for Recommendations A.1 and A.3 of DoDIG Report No. DODIG-2013-134, "Navy Commercial Access Control System Did Not Effectively Mitigate Access Control Risks." Specifically, we determined whether selected Navy installations obtained access to the National Crime Information Center (NCIC) and Terrorist Screening databases, conducted checks of contractor personnel enrolled in the Navy Commercial Access Control System before issuing installation passes, and whether these actions corrected the identified problems.

## Finding

The Commander, Navy Installations Command (CNIC) provided vetting capability to access NCIC as agreed to in Recommendation A.3. However, Navy officials did not properly access NCIC when vetting Navy Commercial Access Control System (NCACS) applicants as agreed to in Recommendation A.1. Specifically, our July 2014 statistical sample results from 945 applicants showed:

- 85 were properly vetted (verified) through NCIC;
- 837 were vetted through Interstate Identification Index (Triple-I); and
- 52 were not vetted through NCIC or Triple-I.

This occurred because CNIC did not provide specific instructions on the appropriate type of queries necessary to access NCIC. Additionally, the reasons for the applicants

### *Finding (cont'd)*

who were not vetted included inadequate use of biographical information when performing background vetting and individuals having manual records.

During our audit, CNIC implemented the OpenFox system, which was to be completed by October 2014. Before implementation, Navy installation officials generally used a query that only accessed Triple-I but not NCIC. In November 2014, we nonstatistically selected a sample of 39 of 250 applicants to review. The results showed that 34 applicants at the six installations that had the OpenFox system implemented were properly vetted through NCIC. All five applicants from one installation, which did not have the OpenFox system implemented, were not properly vetted through NCIC. This installation was under a different network and was waiting for access approval. As of July 2015, the Navy still has 51 of 120 (42.5 percent) of its sites waiting to implement the OpenFox system.

As a result, CNIC was at risk of allowing individuals that may be on NCIC person files to enter Navy installations. This could potentially place military personnel, dependents, civilians, and installations at an increased security risk.

## Recommendations

The Commander, Navy Installations Command should:

- accelerate the implementation of the OpenFox system;
- issue guidance to all installations specifying the queries necessary to access the NCIC person files;
- implement a system control in NCACS to prevent officials from processing NCACS registrations for applicants that have not been vetted through NCIC; and
- require all installations to update their vetting procedures.

## Management Comments and Our Response

Comments from CNIC addressed all specifics of the recommendations, and no further comments are required. Please see the Recommendations Table on the back of this page.

## *Recommendations Table*

| Management | Recommendations Requiring Comment | No Additional Comments Required |
|---|---|---|
| Commander, Navy Installations Command | | 1, 2, 3, 4, and 5 |

**INSPECTOR GENERAL**
**DEPARTMENT OF DEFENSE**
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

November 9, 2015

MEMORANDUM FOR COMMANDER, NAVY INSTALLATIONS COMMAND

SUBJECT: Followup Audit: Navy Access Control Still Needs Improvement
(Report No. DODIG-2016-018)

We are providing this report for your information and use. Although Commander, Navy Installations Command provided the vetting capability to access the National Crime Information Center to all selected Navy installations, Navy installation officials did not properly access it when they performed background vetting as required. We conducted this audit in accordance with generally accepted government auditing standards.

We considered management comments on the draft report when preparing the final report. Comments from the Commander, Navy Installations Command, addressed all specifics of the recommendations and conformed to the requirements of DoD Instruction 7650.03; therefore, we do not require additional comments.

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 604-8905 (DSN 664-8905).

Amy J. Frontz
Acting Deputy Inspector General
for Auditing

# Contents

# Introduction

## Objective

Our objective was to determine whether the identified Navy installations implemented the agreed-upon corrective actions for Recommendations A.1 and A.3 of report DODIG-2013-134, "Navy Commercial Access Control System Did Not Effectively Mitigate Access Control Risks," September 16, 2013. Specifically, we determined whether selected Navy installations obtained access to the National Crime Information Center (NCIC) and Terrorist Screening (TS) databases, conducted checks of contractor personnel enrolled in the Navy Commercial Access Control System (NCACS) before issuing installation passes, and whether these actions corrected the identified problems.

## Background

### *Navy Commercial Access Control System*

NCACS is an access control solution used to manage commercial contractors who require unescorted access to Navy installations. Commander, Navy Installations Command (CNIC) is the office designated to oversee the physical security of Navy installations. CNIC implemented NCACS to comply with DoD security policy and guidance and to improve efficiency and effectiveness at the pass and identification (ID) offices.

Through NCACS, CNIC standardized contractors' enrollment, background vetting, issued and validated credentials, and verified access privileges. NCACS is managed by CNIC and administered through a service provider, Eid Passport. Eid Passport manufactures credentials and maintains information on contractors who access Navy installations. Contractors who seek regular, unescorted access to Navy installations and facilities, and who chose to participate in the NCACS program, do so voluntarily.


Figure 1. Naval Air Station Patuxent River official scans credential for entry.
Source: U.S. Navy, Naval Air Station Patuxent River

## *National Crime Information Center*


Figure 2. Example of an NCACS Card
Source: Commander, Navy Installations Command

To issue the NCACS credentials, Navy officials are required to vet (verify) contractors through the NCIC—a Federal Bureau of Investigation database—to control physical access. DoD Directive 5143.01[1] designates the Office of the Under Secretary of Defense for Intelligence the responsibility to provide policy standards on granting physical access to Federally controlled facilities. USD(I) implemented Directive-Type Memorandum (DTM) 09-012,[2] which states that installation government representatives must query the following government authoritative data sources to vet the identity and determine the fitness[3] of the individual requesting access to the installation:

a. NCIC database;
b. TS database; and
c. other sources as determined by the DoD Component.[4]

USD(I) further issued guidance[5] to DoD Security Directors that specified the minimum criteria, as listed below, to determine the fitness of an individual who seeks unescorted access to a DoD installation but does not have a Federal access card:

a. not on a terrorist watch list;
b. not on an installation debarment list; and
c. not on a felony wants and warrants lists.

Additionally, to implement DTM 09-012, CNIC issued Instruction 5530.14A,[6] which includes entry control standards that require criminal background checks to be performed through NCIC on all contractors and visitors.

[1] DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD[I])," October 24, 2014.
[2] USD(I) Directive-Type Memorandum (DTM) 09-012, "Interim Policy Guidance for DoD Physical Access Control," dated April 22, 2014.
[3] Level of character and conduct necessary to determine whether access would be granted.
[4] We focused on NCIC and TS databases based on our audit objective.
[5] USD(I) memorandum, "National Crime Information Center Check for Non-Federal Government and Non-DoD-Issued Card Holders Seeking Unescorted Access to DoD Installations," November 20, 2013.
[6] CNIC Instruction 5530.14A, "CNIC Ashore Protection Program," May 29, 2013.

NCIC is an electronic database of crime data that can be accessed by every criminal justice agency nationwide, 24 hours a day, 365 days per year. The Criminal Justice Information Services (CJIS) is the central repository for criminal justice information services in the Federal Bureau of Investigation. CJIS has overall responsibility for the administration and usage of the NCIC. The NCIC consists of 14 person files:

1. Known or Appropriately Suspected Terrorist (Suspected Terrorist);[7]
2. Wanted Person;
3. National Sex Offender Registry;
4. Missing Persons;
5. Foreign Fugitive;
6. Identity Theft;
7. Immigration Violator;
8. Protection Order;
9. Supervised Release;
10. Unidentified Persons;
11. Protective Interest;
12. Gang;
13. National Instant Criminal Background Check System Denied Transaction; and
14. Violent Person.

In addition, the Interstate Identification Index (Triple-I) database, which contains automated criminal history record information, is accessible through NCIC. The Triple-I facilitates the interstate exchange of criminal history records among State justice agencies. All 50 states, including the District of Columbia, hold records and provide responses through Triple-I.

According to the Justice Telecommunications System training manual, a vetting official must perform several transactions to access the NCIC person files and criminal history records. Specifically, vetting officials must perform the following queries:

- **QWA**—used to access all NCIC person files, except for Unidentified Person File and National Instant Criminal Background Check System Denied Transaction File.

[7] If a record is located in the Suspected Terrorist File, the Navy official conducting the records check will be referred to the TS Center. Therefore, if the Navy installation officials properly accessed the NCIC, the vetting process would include a check against the TS database.

- **QU**—necessary to access Unidentified Person File.
- **QND**—used to access National Instant Criminal Background Check System Denied Transaction File.
- **QH**—used to access Triple-I (criminal history record).
- **QWI**—used to perform two transactions in one—"QWA" and "QH" queries.

In addition, the NCIC operating manual provides another query option, QW, which can be used for Wanted Person File. A Wanted Person File inquiry will cause an automatic cross-search of the Foreign Fugitive, Missing Person, Gang, Suspected Terrorist, Protection Order, Immigration Violator, Identity Theft, Supervised Release, Violent Person, Protective Interest Files, and National Sex Offender Registry.

### *Vetting Systems*

Navy installation officials used either state vetting systems or the OpenFox system to properly access the NCIC to perform background vetting. Officials would meet the minimum criteria required by USD(I) if they used the QWA, QWI, or QW query. During the audit, CNIC officials started to implement the OpenFox system to standardize the required vetting process throughout the Navy installations. The OpenFox system provides a gateway between state law enforcement information and national information systems, such as the NCIC.

## Review of Internal Controls

DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013, requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. We identified internal control weaknesses related to the NCACS applicants vetting process. Specifically:

- Navy installation officials did not properly access NCIC when performing background vetting as required by the DTM 09-012 and agreed to in Recommendation A.1;
- CNIC guidance did not provide specific instructions on which query would be necessary to ensure the officials properly access the required NCIC person files, including the Suspected Terrorist File; and
- NCACS allowed a Navy installation official to process NCACS applicant's registration before performing a background check.

We will provide a copy of the report to the senior official responsible for internal controls in the CNIC.

# Finding

## Navy Access Control Still Needs Improvement

Even though CNIC provided the vetting capability to access the NCIC to all selected Navy installations as agreed to in Recommendation A.3, Navy installation officials did not properly access the NCIC when performing background vetting as agreed to in Recommendation A.1. Specifically, our July 2014 statistical sample results showed:

- 85 of 945 (9.0 percent) NCACS applicants were properly vetted through NCIC person files;
- 837 of 945 (88.6 percent) NCACS applicants were vetted through Triple-I; and
- 52 of 945 (5.5 percent) NCACS applicants were not vetted through NCIC or Triple-I.

This occurred because CNIC did not provide specific instructions on appropriate type of queries necessary to access the NCIC to ensure all required NCIC person files were checked. Additionally, the reasons for the NCACS applicants who were not vetted included inadequate use of biographical information when performing background vetting and the individuals having manual records.

During our audit, CNIC implemented the OpenFox system to standardize the required vetting process throughout the Navy installations. Before the OpenFox system was implemented, Navy installation officials generally used a query that only accessed the individuals' criminal history files but not all NCIC person files as required when performing background vetting.

According to CNIC officials, the OpenFox system was scheduled for implementation at all sites by October 2014. In November 2014, we nonstatistically selected 39 of 250 NCACS applicants to review. The results showed:

- at the six installations that had the OpenFox system implemented, 34 applicants were properly vetted through NCIC person files; and
- at the one installation that did not have the OpenFox system implemented, all five applicants reviewed were not properly vetted through NCIC person files.

One installation did not have the OpenFox system implemented because it was under a different network and was waiting for approval to access the OpenFox system. As of July 2015, the Navy has 51 of 120 (42.5 percent)[8] of its sites still waiting to implement the OpenFox system.

As a result, CNIC was at risk of allowing individuals that may be on one of the NCIC person files, such as Suspected Terrorist File, to enter Navy installations. This could potentially place military personnel, dependents, civilians, and installations at an increased security risk.

## Audit Summary of DoD OIG Report No. DODIG-2013-134

Numerous contractor employees enrolled in the NCACS received interim installation access and the NCACS credentials without having their identities vetted...

DoD OIG Report No. DODIG-2013-134[9] reported that the NCACS did not effectively mitigate the access control risks of contractors accessing Navy installations. Specifically, numerous contractor employees enrolled in the NCACS received interim installation access and the NCACS credentials without having their identities vetted through mandatory authoritative databases, such as the NCIC and TS databases.

(~~FOUO~~) The results indicated that CNIC did not follow Federal credentialing standards and DoD contractor vetting requirements. Also, CNIC did not provide 7 of the 10 installations under prior audit review with the appropriate resources and capabilities to conduct required contractor background checks. The report identified the following seven installations that granted access to contractor employees without vetting them through NCIC and TS database.

[redacted]

[8] This percentage includes Pass and ID Offices and Dispatch Centers located outside and within the Continental United States. The number used for sites located outside the Continental United States is an estimated number pending the OpenFox system deployment process as some nations may only allow access control background vetting based on the nation's agreement. Some nations may not allow the use of OpenFox system for vetting.

[9] Report DODIG-2013-134 contains three findings. This followup report only focused on Finding A, specifically Recommendations A.1 and A.3.

Figure 3. Official Checks Identification at the Washington Navy Yard.
Source: U.S. Navy

As a result, convicted felons received routine, unauthorized access to Navy installations placing military personnel, dependents, civilians, and installations at an increased security risk.

## *Recommendation A.1 and Agreed-Upon Action*

Recommendation A.1 stated that CNIC should immediately discontinue the use of Rapidgate and any other system that exclusively used publicly available databases to vet and adjudicate contractor employees who access Navy installations and replace it with a system or process that meets Federal and DoD requirements for background vetting.

CNIC agreed and stated that as of September 23, 2013, the Navy officials used the NCIC and TS databases to check all contractors before they issued NCACS credentials to access Navy installations.

...the Navy officials used the NCIC and TS databases to check all contractors before they issued NCACS credentials...

## *Recommendation A.3 and Agreed-Upon Action*

Recommendation A.3 stated that CNIC:

- (~~FOUO~~) provide the resources and capabilities needed to access the NCIC and TS databases to [redacted]

- establish a process to identify which installations need resources and capabilities to access NCIC and TS databases for contractor background vetting and provide installation Commanders with needed resources and capabilities.

CNIC agreed and stated that it provided access control resources and capabilities to all Navy installations. CNIC stated that the specific Navy bases identified in the report have access to the NCIC and TS databases. Also, CNIC indicated that it required all contractors who require physical access to its installations receive the NCIC and TS databases checks prior to receiving interim passes while the full NCACS implementation process is completed.

## Agreed-Upon Action Not Fully Demonstrated

Even though CNIC provided the vetting capability to access NCIC to all selected Navy installations as agreed to in Recommendation A.3, Navy installation officials did not properly conduct background checks through the NCIC database for all contractors requesting access to Navy installations, as required by DTM 09-012 and agreed to in Recommendation A.1.

### *Vetting Capability Provided*

CNIC provided the vetting capability to access NCIC to the selected seven Navy installations as agreed to in Recommendation A.3. DTM 09-012 requires that installation officials vet individuals through NCIC and TS databases. The selected Navy installations either had local terminals that could access the NCIC through their state systems or the OpenFox system. For those installations that lacked local access to the NCIC, they could use other remote installations to access the NCIC.

CNIC provided the vetting capability to access NCIC to the selected seven Navy installations...

(~~FOUO~~) For example, in July 2014, before CNIC implemented the OpenFox system, installation officials at [redacted] used Maryland Electronic Telecommunications Enforcement Resource System to perform background vetting. Officials at the [redacted] used [redacted] to remotely perform background vetting through Mississippi Justice Information Center. Officials at the [redacted] used Automated Regional Justice Information System to perform background vetting for the [redacted]. Lastly, officials at the [redacted] used Washington State Patrol Service to perform background vetting for [redacted].

(~~FOUO~~) By September 2014, six of seven installations in our review implemented the OpenFox system. As of July 2015, the [redacted] still used the Maryland Electronic Telecommunications Enforcement Resource System to perform background vetting. Therefore, the seven selected Navy installations had the capability to properly access the NCIC person files, including the Suspected Terrorist File, to perform background vetting if they used the appropriate query.

## *National Crime Information Center Not Properly Accessed as Required*

Navy installation officials did not properly access NCIC as required by DTM 09-012 and agreed to in Recommendation A.1. According to DTM 09-012, installation government representatives shall query the NCIC database, the TS database, and other data sources by the DoD Component to vet the claimed identity and to determine fitness, using biographical information.

Navy installation officials did not properly access NCIC as required by DTM 09-012...

NCIC consists of 14 person files, which include the Suspected Terrorist File and Wanted Person File. To access the NCIC person files, Navy officials must perform a QWA, QWI, or QW query to meet the minimum criteria required by the USD(I). If Navy officials only performed a QH query, they would only access the criminal history record through Triple-I, not NCIC. Triple-I contains criminal history records from State justice agencies; it does not contain other person files, such as Suspected Terrorist File and Wanted Person File, as NCIC does.

We selected two samples to determine whether Navy officials were properly vetting NCACS applicants—one for the month of July 2014 and a smaller sample for the week of November 2014 due to a change in CNIC vetting process.

### *Prior to OpenFox System Implementation*

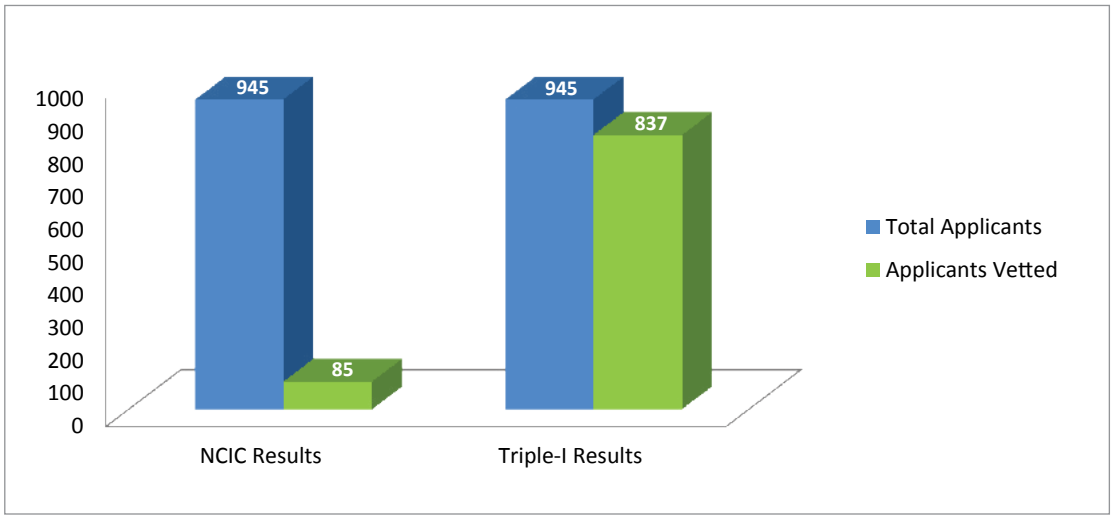
...only 85 (9.0 percent) were properly vetted through NCIC person files.

We statistically selected a sample of 180 of 945 NCACS applicants from the seven installations who received NCACS credentials in July 2014.[10] Of the 945 NCACS applicants, only 85 (9.0 percent) were properly vetted through NCIC person files. Also, of the 945 applicants, 837 (88.6 percent) were vetted through Triple-I because the officials used the QH query, which only accessed criminal history records.

[10] See Appendix B for more details on our universe and how we selected our sample.

Figure 4 below shows the result of the NCIC person files and criminal history records that Navy officials accessed during our review of the July 2014 sample.

*Figure 4. Result of NCACS Applicants Vetted Through NCIC and Triple-I*




Source: DoD OIG

During July 2014, most of the selected installations used state systems for background vetting. According to installation officials, state officials instructed them to use the QH query[11] to access individuals' criminal history through their state systems. If there was any indication of an unfavorable result, they would access the individual's rap sheet[12] to obtain additional information. The officials at the selected installations were not aware that the QH query would not access the NCIC person files.

Installation officials did not perform background vetting through either NCIC or Triple-I for 52 of 945 (5.5 percent) NCACS applicants.

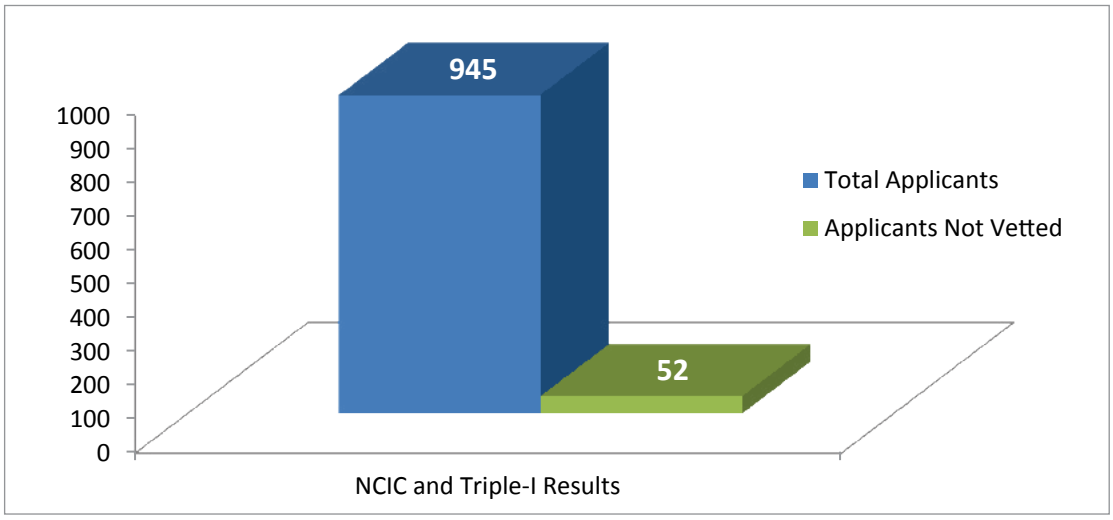
In addition, installation officials did not perform background vetting through either NCIC or Triple-I for 52 of 945 (5.5 percent) NCACS applicants. We determined an applicant was not vetted if the applicant's name, social security number or date of birth, and the Originating Agency Identifier[13] provided by CNIC, did not match with the information on the reverse check from NCIC and Triple-I provided by CJIS. Figure 5 below shows the result of the NCACS applicants that were not vetted through either NCIC or Triple-I.

[11] According to Navy officials, they would also use a master query in their state vetting systems but the standard process would be to perform the QH query. We observed that the master query would not provide as much detail as a QH or QWI query.

[12] A rap sheet query is performed to obtain a specific criminal history record through Triple-I.

[13] The Originating Agency Identifier is a nine character number assigned by CJIS to an agency in order to have access to NCIC and Triple-I.

*Figure 5. Result of NCACS Applicants Not Vetted Through NCIC or Triple-I*




Source: DoD OIG

(~~FOUO~~) In some cases, Navy officials did not adequately use multiple biographical information, such as the individual's name, date of birth, and social security number when they performed background vetting through NCIC or Triple-I. For example, officials at [redacted] only used the name and date of birth to vet an individual in our sample. According to the installation officials, they vetted this individual. However, both the individual's name and date of birth did not match the reverse check record that we obtained from CJIS. The only information that matched was the individual's name. Thus, the individual that they vetted may not be the same individual in our sample. As best practice, installation officials should at least use the individual's name, date of birth, and social security number as a minimum when vetting to reduce the risk of accessing the information of another person.

In other cases, individuals were not vetted through either NCIC or Triple-I because installation officials automatically determined the individuals to be unfavorable when a manual record was found for that individual when searching the state system, and therefore, access would be denied. Installation officials would then request the applicant to retrieve his or her own criminal history record and submit it for further evaluation to determine whether access should be granted.

(~~FOUO~~) The lack of personnel resources may also have contributed to some of the applicants that were not vetted. For example, the [redacted] had only two vetting officials, and they had over 2,900 individuals to vet for the months of July and August 2014. Our sample results showed that [redacted] had the

(~~FOUO~~) highest number of applicants not vetted per total applicants. One vetting official indicated that the [redacted] had initiated an internal audit to identify the reasons why these individuals were not vetted prior to granting access.

Furthermore, NCACS allowed officials to process the applicant's registration before they performed background vetting to determine their fitness for installation access. CNIC should develop and implement a system control in NCACS to prevent officials from processing an applicant's registration if the applicant has not been vetted through NCIC.


### *After OpenFox System Was Implemented*

During our audit, CNIC implemented the OpenFox system to improve background vetting. We nonstatistically selected a sample of 39 of 250 NCACS applicants for the week of November 17–21, 2014, from the selected seven installations to determine whether implementing the OpenFox system would ensure Navy installation officials properly accessed the NCIC person files when they conducted background vetting.

(~~FOUO~~) The result showed that at the six installations that implemented the OpenFox system, 34 NCACS applicants were properly vetted through NCIC person files. Officials at these installations properly used the QWA, QWI, or QW query to access the NCIC person files. At the [redacted], which did not have the OpenFox system implemented, all five applicants reviewed were not properly vetted through NCIC person files. The [redacted] did not use the QWA, QWI, or QW query when using the state system to access NCIC.

If they do not use proper queries to access NCIC, installation officials may not be able to access appropriate person files to properly conduct background vetting. As a result, it could potentially place Navy installations at risk of allowing individuals that may be on the NCIC person files, specifically the Suspected Terrorist File, to enter the Navy installations.

(~~FOUO~~) As of July 2015, the [redacted] still used the state system to conduct background vetting. According to CNIC officials, [redacted] was under a different network and was waiting for approval to access OpenFox system. However, officials at the [redacted] revised their standard operating procedures, dated May 26, 2015, to include a requirement to use QWI query when performing background vetting.

In addition, CNIC officials indicated that all Navy installations would have the OpenFox system implemented by October 2014. However, as of July 2015, CNIC OpenFox system implementation plan showed that only 69 of 120 (57.5 percent) of sites located on Navy installations had the OpenFox system. CNIC should accelerate the implementation of the OpenFox system for all Navy Pass and ID Offices and Dispatch Centers.


## *CNIC Guidance Not Adequate*

DTM 09-012 requires installation officials to access the NCIC and TS databases to determine the fitness of individuals who request unescorted access to DoD installations. To comply with DTM 09-012, CNIC developed guidance to conduct background vetting for Navy installations. CNIC guidance provided more specific instructions, implemented best practices, and provided requirements and direction for the protection of people and assets.

For example, the instructions included a provision that being on the Suspected Terrorist File is the ground for access denial. However, the CNIC guidance did not provide specific instructions on which query is necessary to ensure the officials properly access all the required NCIC person files, including Suspected Terrorist File.

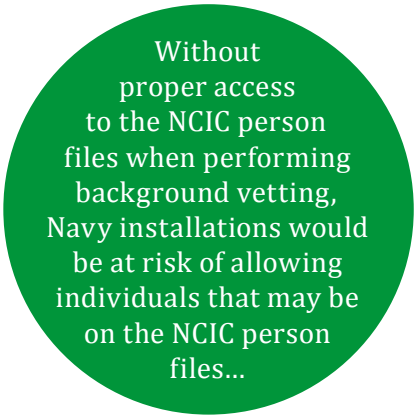
In addition, all selected Navy installations had standard operating procedures to conduct background vetting. However, the standard operating procedures at four out of the seven selected Navy installations did not specify the queries necessary to properly access the NCIC person files as required. CNIC should require all installations officials to update their standard operating procedures to include specific instruction to access the NCIC person files.

CNIC officials stated that the OpenFox system would minimize improper background vetting. According to CNIC officials, they provided the OpenFox system training and instructed vetting officials to perform the QWI query. However, the OpenFox system was not implemented at all Navy installations as of July 2015.

For the offices that did not have the OpenFox system for background vetting, officials may not have used the proper queries when using the state systems. Without the specific instructions on which queries are necessary to access NCIC, installation officials may not have properly accessed the NCIC person files as required.

(~~FOUO~~) In November 2014 and February 2015, the audit team informed CNIC officials about installations that did not have the OpenFox system implemented may still use QH query to conduct background vetting, such as [redacted] As of August 2015, CNIC officials still did not have guidance on specific queries to properly access the NCIC to installations that did not have the OpenFox system implemented.

Without proper access to the NCIC person files when performing background vetting, Navy installations would be at risk of allowing individuals that may be on the NCIC person files, specifically the Suspected Terrorist File, to enter Navy installations. This could potentially place military personnel, dependents, civilians, and installations at an increased security risk.




## Conclusion

CNIC officials provided vetting capabilities to access NCIC to the seven selected installations as agreed to in Recommendation A.3. However, CNIC did not provide guidance on specific queries necessary to properly access the required NCIC person files as agreed to in Recommendation A.1. Without specific instructions on which queries are necessary to access NCIC, installation officials, specifically at Navy installations that did not have OpenFox system and still used state systems, may not have properly accessed the NCIC person files as required. As of July 2015, the Navy still had 51 of 120 (42.5 percent) of its sites waiting to implement the OpenFox system.

## Recommendations, Management Comments, and Our Response

### *Recommendation 1*

**We recommend that Commander, Navy Installations Command accelerate the implementation of the OpenFox system for all Navy Pass and ID Offices and Dispatch Centers.**

#### *Commander, Navy Installations Command Comments*

The Commander, Navy Installations Command, agreed, stating that the command will initiate a program to expedite the implementation of OpenFox system access to the remainder of the enterprise. He anticipates that this will be completed no later

than January 1, 2016. In the interim, the Commander will ensure that installations without OpenFox or NCIC access are supported by other regions or installations with access to complete the required vetting of contractors or unaffiliated visitors.

### *Our Response*

Comments from the Commander addressed all specifics of the recommendation, and no further comments are required.

## *Recommendation 2*

**We recommend that Commander, Navy Installations Command issue guidance to all installations officials specifying the use of QWA, QWI, QW, or any updated queries, as applicable, to access the National Crime Information Center person files.**

### *Commander, Navy Installations Command Comments*

The Commander, Navy Installations Command, agreed, stating that CNIC Instruction 5530.14A is being updated to address this previous oversight and is anticipated to be completed by October 30, 2015. The updated Instruction will direct Government personnel responsible for the vetting of contractor and unaffiliated visitors to complete an NCIC "QWI" or "QWA" query.

### *Our Response*

Comments from the Commander addressed all specifics of the recommendation, and no further comments are required.

## *Recommendation 3*

**We recommend that Commander, Navy Installations Command develop and implement a system control in Navy Commercial Access Control System to prevent installation officials from processing the Navy Commercial Access Control System registration for applicants that have not been vetted through the National Crime Information Center.**

### *Commander, Navy Installations Command Comments*

The Commander, Navy Installations Command, agreed, stating that the command will develop the process to ensure that only contractors who have been properly vetted in accordance with the DTM 09-012 and CNIC Instruction 5530.14A are issued NCACS credentials. The issuing authority at the visitor control center will be directed to verify that the identity and fitness of the NCACS participant has been proofed and vetted prior to the issuance of the credential.

### *Our Response*

Comments from the Commander addressed all specifics of the recommendation, and no further comments are required.

## *Recommendation 4*

**We recommend that Commander, Navy Installations Command require all installations officials to update their standard operating procedures to include instruction on the use of QWA, QWI, QW, or any updated queries, as applicable, to access the National Crime Information Center person files.**

### *Commander, Navy Installations Command Comments*

The Commander, Navy Installations Command, agreed, stating that the updated CNIC Instruction 5530.14A will require Regions and Installations to update their local directives to comply with installation access control. This action will ensure that Government personnel who are responsible for the vetting of contractor and unaffiliated visitors complete an NCIC "QWI" or "QWA" query.

### *Our Response*

Comments from the Commander addressed all specifics of the recommendation, and no further comments are required.

## *Recommendation 5*

**We recommend that Commander, Navy Installations Command require all installation officials to update their standard operating procedures to include the use of applicant's name, date of birth, and social security number as a minimum standard of biographical information required for vetting.**

### *Commander, Navy Installations Command Comments*

The Commander, Navy Installations Command, agreed, stating that the command will direct the requirement to use at least one additional numeric identifier in addition to name and date of birth when performing vetting.

### *Our Response*

The Commander, Navy Installations Command, agreed and recognized the value in adding additional numeric identifiers when performing vetting. However, instead of using the applicant's social security number specifically as an additional identifier, the Commander will require vetting officials to use at least one other numeric identifier in addition to name and date of birth when performing vetting. This new requirement meets the intent of our recommendation. Therefore, no further comments are required.

# Appendix A

## Scope and Methodology

We conducted this performance audit from July 2014 through September 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We selected seven Navy installations identified in Recommendations A.1 and A.3 of DoD OIG Report No. DODIG-2013-134. The locations were:

We visited the pass and ID offices at the selected installations in August and September 2014 to observe vetting procedures and identify the vetting terminals. We also interviewed personnel from Physical Security Office of the Under Secretary of Defense for Intelligence and Eid Passport.

We collected, reviewed, and analyzed vetting support documentation that included reverse check reports from NCIC and Triple-I databases; state vetting system contracts; installations' standard operating procedures; and additional support obtained through meetings and emails. We compared vetting support documentation to applicable physical access control regulations and system manuals that included:

- DoD Directive 5143.01, "Under Secretary of Defense for Intelligence," October 24, 2014;
- DTM 09-012, "Interim Policy Guidance for DoD Physical Access Control," December 8, 2009, incorporating change 4 effective April 22, 2014;

- Office of the USD(I) Memorandum for DoD Security Directors, "National Crime Information Center Check for Non-Federal Government and Non-DoD-Issued Card Holders Seeking Unescorted Access to DoD Installations," November 20, 2013;
- CNIC Instruction 5530.14A, "CNIC Ashore Protection Program," May 29, 2013;
- U.S. Department of Justice – Justice Telecommunications System Training Manual, January 2015; and
- Federal Bureau of Investigation – NCIC Operating Manual, July 2013.

To determine whether Navy officials properly vetted individuals, we selected two samples. First, we statistically selected a sample of 180 of 945 individuals from the seven selected installations who received credentials in July 2014.[14] After CNIC started to implement the OpenFox system, we determined whether implementing the OpenFox system would ensure that Navy installation officials properly access the NCIC person files when conducting background vetting.

We used the Microsoft Excel random number generator to nonstatistically select a second sample of 39 of 250 NCACS applicants from the selected seven installations who received credentials for the week of November 17 through 21, 2014.

## Use of Computer-Processed Data

We obtained and used computer-processed data. Specifically, we obtained the total number of NCACS applicants from Rapidgate[15] and the reverse check from NCIC and Triple-I. We used the reverse check from NCIC and Triple-I, provided by CJIS, to validate the information obtained from Rapidgate, which was provided by CNIC. We also used NCIC data to validate the data from Triple-I and vice versa. As a result, we determined that the data used were sufficiently reliable for the purpose of this audit.

## Use of Technical Assistance

We obtained support from the DoD OIG Quantitative Methods Division (QMD) to develop the statistical sample of NCACS applicants for the month of July 2014. See Appendix B for more details on our universe and how we selected our sample.

[14] See Appendix B for more details on our universe and how we selected our sample.

[15] Rapidgate is Eid Passport's access control system used to process the NCACS credentials.

## Prior Coverage

During the last 5 years, the DoD Office of the Inspector General (DoD IG) issued one report related to the NCACS access control. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/pubs/index.cfm.

### *DoD IG*

~~(FOUO)~~ [redacted]

# Appendix B

## QMD Sample Design for NCACS Applicants

QMD developed a sample design from the population of NCACS applicants for the seven selected Navy installations.

### *Population*

CNIC provided the total number of credentials issued to NCACS applicants from Rapidgate for the month of July 2014. We grouped the NCACS applicants by installations and determined that an individual that applied for and received an NCACS credential from Eid Passport would be counted as part of the universe. There were 945 contractors that Eid Passport had shipped their NCACS credential.

### *Measures*

We used an attribute[16] measure of the sample design as "pass" for those individuals that were vetted through NCIC and Triple-I or "fail" for those individuals that were not vetted through NCIC and Triple-I.

### *Parameters*

We used a 90-percent confidence level to estimate the sample sizes and projections. For the attribute design, we used the worst-case rate, 50-percent error, for planning purposes.

### *Sample Design*

We performed a stratified attribute design to stratify (group) the universe by the seven locations selected for review. We selected a statistical random sample of 180 of 945 applicants with a 90-percent confidence level. We used the RAND function in Microsoft Excel to randomize each stratum and randomly selected the corresponding sample items without replacement based on the sample size. See Table B-1 for the NCACS applicants' universe and sample selection at each of the seven Navy installations.

[16] A characteristic that is measured to determine whether it meets a specific standard.

*Table B-1. NCACS Applicants Population and Sample Selection*

| Installation Name | Population Size | Sample Size |
|---|---|---|
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |

## *Statistical Projections and Interpretation*

We performed stratified projection at the 90-percent confidence level[17] based on our sample results. Table B-2 below describes the statistical projection and the associated error rates of individuals that were vetted through NCIC.

*Table B-2. Projected Number of Errors and Error Rates for NCIC Vetted (NCIC Person Files), Triple-I-Vetted (Criminal History) and Both NCIC & Triple-I-Not Vetted (Not Vetted in NCIC Person File and Criminal History).*

| Category | Number of Errors | | | Error Rate Percent | | |
|---|---|---|---|---|---|---|
| | Lower Bound | Point Estimate | Upper Bound | Lower Bound | Point Estimate | Upper Bound |
| NCIC Vetted* | 44 | 85 | 126 | 4.7 | 9.0 | 13.3 |
| Triple-I-Vetted* | 782 | 837 | 893 | 82.8 | 88.6 | 94.5 |
| Both NCIC & Triple-I-Not Vetted | 13 | 52 | 91 | 1.3 | 5.5 | 9.7 |

* These numbers do not add up to 945 NCACS applicants in our universe because the number of applicants vetted in NCIC may overlap with the number of applicants vetted in Triple-I.

[17] The formula used in the projections is from the basic formula given in "Sampling Techniques" by William F. Cochran, 3rd edition, pp. 56-58, 91-95, and 107-108.

# Management Comments

## CNIC Comments

THE DEPUTY UNDER SECRETARY OF THE NAVY
WASHINGTON DC 20350-1000

OCT 2 1 2015

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Navy Commercial Access Control System Did Not Effectively Mitigate Access Control Risks

The Department of the Navy (DON) appreciates the opportunity to comment and respond to the recommendations from the Department of Defense Inspector General's Follow-up Audit Report, Navy Access Control Still Needs Improvement dated September 4, 2015.

There were five recommendations for Navy Commercial Access Control System (NCACS) program to improve reliability and consistency of identity proofing and vetting of commercial vendors and non-CAC eligible cardholders at installations.

Commander, Navy Installations Command has responded to those recommendations with an action plan and the DON concurs with their response, which is attached.

My point of contact for this matter is [redacted] or email: [redacted]

Jodi Greene

Attachment:
As stated

## CNIC Comments (cont'd)

DEPARTMENT OF THE NAVY
COMMANDER, NAVY INSTALLATIONS COMMAND
716 SICARD STREET, SE, SUITE 1000
WASHINGTON NAVY YARD, DC 20374-5140

5740
Ser N00G/15U1062
25 Sep 15

From: Commander, Navy Installations Command
To: Acting Deputy Inspector General for Auditing, Inspector General, Department of Defense

Subj: DRAFT REPORT RESPONSE TO FOLLOWUP AUDIT: NAVY ACCESS CONTROL STILL NEEDS IMPROVEMENT (PROJECT NO. D2014-D000XD-0194.000)

Ref: (a) DoD IG memo of 4 Sep 15

Encl: (1) CNIC Draft Report Response

1. Per reference (a), Commander, Navy Installations Command (CNIC) has reviewed the Draft Report. Specific comments are provided in enclosure (1).

2. The technical point of contact is [redacted]

GERALD R. MANLEY
By direction

Copy to:
CNIC (N00, N00L, N3)

## CNIC Comments (cont'd)

COMMANDER, NAVY INSTALLATIONS COMMAND
DRAFT REPORT RESPONSE TO
FOLLOWUP AUDIT: NAVY ACCESS CONTROL
STILL NEEDS IMPROVEMENT
(PROJECT NO. D2014-D000XD-0194.000)

Commander, Navy Installations Command's (CNIC's) responses to the findings and recommendations of the Department of Defense Inspector General's (DoD IG's) subject Draft Report are provided below. CNIC concurs with the recommendations.

**Recommendation 1**: Accelerate the implementation of the OpenFox system for all Navy Pass and ID Offices and Dispatch Centers.

**Response**: Concur. CNIC will initiate a program to expedite the implementation of OpenFox system access to the remainder of the enterprise. We anticipate this being completed no later than 1 January 2016. In the interim CNIC will ensure installations which do not have access to OpenFox or National Crime Information Center (NCIC) to complete the required vetting of contractors or unaffiliated visitors are supported by other regions or installations with access to OpenFox.

**Recommendation 2**: Issue guidance to all installation officials specifying the use of QWA, QWI, QW, or any updated queries, as applicable, to access the NCIC person files.

**Response**: Concur. CNIC is currently updating CNICINST 5530.14A to address this previous oversight and anticipates promulgation of the change by 30 October 2015. The change will direct that Government personnel responsible for the vetting of contractor and unaffiliated visitors complete an NCIC "QWI" or "QWA" query.

**Recommendation 3**: Develop and implement a system control in Navy Commercial Access Control System (NCACS) to prevent installation officials from processing the NCACS registration for applicants who have not been vetted through the NCIC.

**Response**: Concur. CNIC will further develop the process to ensure only contractors who have been properly vetted to the DTM 09-12 and updated CNICINST 5530.14A are issued NCACS credentials no later than 30 October 2015. The issuing authority at the Visitor Control Center (VCC) will be directed to verify the NCACS participant has been identity proofed, vetted, and appropriate fitness determination has been completed prior to the issuance of the credential.

**Recommendation 4**: Require all installation officials to update their standard operating procedures to include instruction on the use of QWA, QWI, QW, or any updated queries, as applicable, to access the NCIC person files.

**Response**: Concur. CNIC, with the promulgation of the update to CNICINST 5530.14A, will require regions and installations to update their local directives to ensure compliance with installation access control no later than 30 October 2015. This action will ensure Government personnel responsible for the vetting of contractor and unaffiliated visitors complete an NCIC QWI or QWA query.

**Recommendation 5**: Require all installation officials to update their standard operating procedures to include the use of applicant's name, date of birth, and social security number as a minimum standard of biographical information required for vetting.

Enclosure (1)

## CNIC Comments (cont'd)

**Response:** Concur with Intent. The required information necessary to conduct a QWI or QWA query in NCIC is the applicant's name and date of birth. However, we recognize the value in adding other numeric identifiers such as social security number, operator license number, passport number, etc. and will direct the requirement for at least one additional numeric identifier in addition name and date of birth no later than 30 October 2015.

2

Enclosure (1)

# Acronyms and Abbreviations

| | |
|---|---|
| **CJIS** | Criminal Justice Information Services |
| **CNIC** | Commander, Navy Installations Command |
| **DTM** | Directive-Type Memorandum |
| **ID** | Identification |
| **NCACS** | Navy Commercial Access Control System |
| **NCIC** | National Crime Information Center |
| **QMD** | Quantitative Methods Division |
| **TS** | Terrorist Screening |
| **Triple-I** | Interstate Identification Index |
| **USD(I)** | Under Secretary of Defense for Intelligence |

# Whistleblower Protection
## U.S. Department of Defense

*The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit www.dodig.mil/programs/whistleblower.*

## For more information about DoD IG reports or activities, please contact us:

**Congressional Liaison**
congressional@dodig.mil; 703.604.8324

**Media Contact**
public.affairs@dodig.mil; 703.604.8324

**Monthly Update**
dodigconnect-request@listserve.com

**Reports Mailing List**
dodig_report@listserve.com

**Twitter**
twitter.com/DoD_IG

**DoD Hotline**
dodig.mil/hotline

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098