REPORT OF INVESTIGATION

SUBJECT	CASE NUMBER
(b) (6), (b) (7)(C), (b) (7)(F) Acting Chief Deputy United States Marshal (b) (6), (b) (7)(C) [redacted]	(b) (6), (b) (7)(C) [redacted]

OFFICE CONDUCTING INVESTIGATION	DOJ COMPONENT
Chicago Field Office	United States Marshal Service

DISTRIBUTION	STATUS
☒ Field Office CFO	☐ OPEN ☐ OPEN PENDING PROSECUTION ☒ CLOSED
☒ AIGINV	PREVIOUS REPORT SUBMITTED: ☐ YES ☒ NO
☒ Component USMS	Date of Previous Report:
☐ USA	
☐ Other	

SYNOPSIS

The Department of Justice (DOJ) Office of the Inspector General (OIG) initiated this investigation upon the receipt of information from the United States General Services Administration (GSA) alleging that (b) (6), (b) (7)(C) [redacted] to (b) (6), (b) (7)(C), United States Marshals Service (USMS) Acting Chief Deputy United States Marshal (b) (6), (b) (7)(C), (b) (7)(F) (b) (6), (b) (7)(C) [redacted]

(b) (6), (b) (7)(C) [redacted]

During the course of the investigation, the OIG found indications that (b) (6), (b) (7)(C), (b) [redacted] may have failed to safeguard sensitive contract information by providing (b) (6), (b) [redacted] with (b) (6), (b) (7)(C) information related to the (b) (6), (b) (7)(C) project. The OIG investigation substantiated the allegation that (b) (6), (b) (7)(C), (b) [redacted] failed to safeguard sensitive contract

DATE January 11, 2021	SIGNATURE (b) (6), (b) (7)(C) [redacted]
(b) (6), (b) (7)(C) [redacted] PREPARED BY SPECIAL AGENT	
DATE January 11, 2021	SIGNATURE William Hannah Digitally signed by WILLIAM HANNAH Date: 2021.01.11 15:56:33 -06'00'
William J. Hannah APPROVED BY SPECIAL AGENT IN CHARGE	

information by providing [redacted] with [redacted] information, which included [redacted] and other contractors' proprietary information related to the [redacted] project, [redacted] in violation of USMS policy.

[redacted] told the OIG that [redacted] emailed him some pricing information from [redacted] contract on the [redacted] project. [redacted] did not recall if the information he received included [redacted] estimate and contracts. [redacted] believed that [redacted] was doing market research to see if the USMS was getting fair and equitable pricing from [redacted] through [redacted] contract, [redacted]

All of the other witnesses interviewed had no direct, personal knowledge that [redacted] provided [redacted] with the [redacted] contract or bid information and documents for the [redacted] project. [redacted] All the witnesses denied receiving contract, bid information, or other related documents from [redacted], except for [redacted]. [redacted]

[redacted]

The OIG reviewed [redacted] USMS e-mail and discovered that on [redacted], [redacted] forwarded an e-mail he received from [redacted] on [redacted], to [redacted] This e-mail contained a summary of the pricing information and documentation for the [redacted] project [redacted] to [redacted] The documents contained the following markings: "For Official Use Only" and "This proposal includes data that shall not be disclosed outside [redacted]. and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than to evaluate this proposal."

During an OIG interview, [redacted] admitted to forwarding the aforementioned e-mail to [redacted] because he believed the initial estimate by [redacted] for the [redacted] project was unreasonable. [redacted] said that he sent the [redacted] project estimate to [redacted] in order to verify that the price estimate the USMS received from [redacted] was fair and reasonable. [redacted] said he believed that because [redacted] told him that they no longer wanted to be part of the market research and that it was [redacted] for them, that it was "okay" to ask [redacted] to verify the price estimate. Therefore, he sent them the [redacted] information for the [redacted] project [redacted] acknowledged that the release of a competitor's business strategy had the potential to create an unfair advantage or disadvantage for the companies involved. [redacted]

The DOJ Public Integrity Section declined to open an investigation related to this matter.

The OIG has completed its investigation and is providing this report to the USMS for appropriate action.

Unless otherwise noted, the OIG applies the preponderance of the evidence standard in determining whether DOJ personnel have committed misconduct. The Merit Systems Protection Board applies this same standard when reviewing a federal agency's decision to take adverse action against an employee based on such misconduct. See 5 U.S.C. § 7701(c)(1)(B); 5 C.F.R. § 1201.56(b)(1)(ii).

DETAILS OF INVESTIGATION

Predication

The Department of Justice (DOJ) Office of the Inspector General (OIG) initiated this investigation upon the receipt of information from the United States General Services Administration (GSA) alleging that [redacted] United States Marshals Service (USMS) Acting Chief Deputy United States Marshal [redacted] The OIG conducted this investigation jointly with the GSA OIG.

During the course of the investigation, the OIG found indications that [redacted] may have also failed to safeguard sensitive information by providing [redacted] information, which included [redacted] and other contractors' proprietary information for the [redacted] project [redacted]" to [redacted]

Investigation Process

The OIG's investigative efforts consisted of the following:
Interviews and Discussions with the following USMS employees:

- [redacted], Acting Chief Deputy United States Marshal
- [redacted]

Interviews of the following [redacted] employees:

[redacted]

Interviews of the following GSA employees:

[redacted]

Review of the following:

- [redacted] USMS e-mail
- [redacted] training history

Background

Around [redacted] was awarded [redacted] was a [redacted] subcontractor of the contract. GSA was the contracting agency for the government for this project and the USMS was the client of GSA. Acting Chief Deputy United States Marshal [redacted] was the authorizing official for USMS on this contract because it was in his district. [redacted] provided GSA with the projects that the USMS wanted completed and was also the authorizing official for the projects. Toward the end of the project, the USMS was notified that there was unspent money on the contract. The USMS attempted to use the money for other small projects in the building that fit the scope of the initial contract, which were considered change orders to the existing contract. One of the projects that the USMS asked to have completed was [redacted] The USMS expressed its desire to have this project completed under [redacted], which GSA agreed was within the scope of the contract. GSA asked [redacted] to provide a price estimate for the [redacted] project. [redacted] provided an estimate [redacted]. The USMS made some changes to the project in an attempt to reduce the cost, such as completing the work during business hours. In addition, GSA researched cost savings efforts related to the project.

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

(b) (6), (b) (7)(C), (b) (7)(F) Failure to Safeguard Sensitive Information

During the course of the investigation, the OIG found indications that (b) (6), (b) (7)(C), (b) may have failed to safeguard sensitive information by providing (b) (6), (b) (7)(C) information, which included (b) (6), (b) (7)(C) and other contractors' proprietary information, for the (b) (6), (b) (7)(C) project (b) (6), (b) (7)(C) to (b) (6), (b) (7

USMS Policy Directives, Tactical Operations, 17.6.3 Document Security Policy states in pertinent part:

> Section F "Procedures," Subpart 7 "For Official Use Only (FOUO)":
>
> For Official Use Only (FOUO):
>
> f. FOUO information used by the USMS must be maintained, distributed, secured, and disposed of in a manner that will protect the information against unauthorized disclosure. FOUO information is unclassified information of a sensitive, proprietary, or personally private nature which must be protected against release to unauthorized individuals. This term is prescribed for use within DOJ and the USMS to signify and identify such information and is the preferred marking for material that could alternatively be marked LOU or LES.
>
> g. The following categories of information are designated as FOUO information and must be marked accordingly:
>
> 1. Sensitive information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA) 5 U.S.C. §552, although the marking itself does not create an exemption;
>
> ...
>
> 4. Memoranda or reports that disclose security vulnerabilities;
>
> ...
>
> 6. Company proprietary information;
>
> ...
>
> 11. Pre-award contracting information.

Section F "Procedures," Subpart 8 "Procedures for Sensitive But Unclassified Information (LES/LOU/FOUO)":

> Procedures for Sensitive But Unclassified Information (LES/LOU/FOUO):
>
> a. The USMS Director is authorized to determine which categories of information, in addition to the above, should require additional protective measures.
> b. Unclassified information that has been determined to required protection against unauthorized disclosure must be identified as LOU/LES/FOUO to ensure all persons having access to the information are aware of the protection requirement. The method of identification of sensitive:
>
> ...
>
> 3) FOUO material is to be marked "FOR OFFICIAL USE ONLY" on the first page of the material. Documents must also contain "U/FOUO" in the header and footer of each page. Material containing FOUO information may further be identified by the use of Form USM-5B, For Official Use Only Cover Sheet.
>
> c. Sensitive material transmitted by email must include the appropriate marking in the SUBJECT line of the message (e.g., U/LES")
>
> ...
>
> e. Personnel who have custody of material designated as sensitive must exercise due caution to ensure the information is not available to individuals who do not have a need to know. At a minimum, unauthorized individuals must not be able to enter areas unobserved and gain visual access to sensitive information
>
> ...
>
> i. Information which has been identified and is known by the recipient as LOU/LES/FOUO will be safeguarding from disclosure to unauthorized individuals whether or not the material is physically marked. Safeguarding from disclosure includes precautions against oral disclosure, prevention of visual access to the information, and precautions against release of the material to unauthorized personnel.
>
> ...
>
> m. If sensitive information must be released to non-government personnel as part of a contract or grant, those personnel must have a need to know and a favorably adjudicated background investigation of the same scope as is required for USMS employees, prior to being granted access to the sensitive information
>
> ...

The OIG's review of [redacted] USMS e-mail revealed that on (b) (6), (b) (7)(C) [redacted] sent [redacted] the [redacted] contract related to the project (b) (7)(E) [redacted] via e-mail. The information that [redacted] released to [redacted] included documents marked "For Official Use Only" and documents marked "This proposal includes data that shall not be disclosed outside (b) (6), (b) (7)(C) [redacted] and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than to evaluate this proposal." These documents contained proprietary information from numerous private companies involved in (b) (7)(E) [redacted] contract. The proprietary information included: pricing for materials, pricing for design and construction, labor costs, description of work to be completed, and proposals of costs for different tasks. These documents are very detailed and explain how each company arrived at their costs, which could include a company's competitive advantage over other companies.

The OIG discussed USMS policy with USMS [redacted] who stated that he believed [redacted] violated USMS document security policy by providing another company's proprietary information to a potential competitor. [redacted] believed that the USMS has the responsibility to honor a company/vendor's proprietary

information and ensure it is not disclosed to a potential competitor. [redacted] believed that if the company/vendor's documents had "For Official Use Only" markings or requests non-disclosure of their information, the USMS policy requires USMS officials to abide by those requests or re-engage with the company to be released from the requirement.

[redacted] told the OIG that he recalled forwarding an e-mail that he received from USMS [redacted] to [redacted], which contained pricing information and possibly the documents for the [redacted] project. [redacted] did not recall if he brought paperwork with him to the initial meeting, but definitely did not believe he left paperwork with [redacted] acknowledged that the release of a competitor's business strategy had the potential to create an unfair advantage or disadvantage for the companies involved.

OIG's Conclusion

The OIG investigation concluded that [redacted] failed to exercise due caution to ensure sensitive information was unavailable to individuals who did not have a need to know and his actions constituted administrative misconduct in violation of USMS Policy Directives, Tactical Operations, 17.6.3, Document Security Policy, Section F, and was an unauthorized release of information. The email evidence in this investigation shows that [redacted] shared [redacted] proprietary information to [redacted] and [redacted] admitted to forwarding the proprietary information of [redacted] to [redacted]