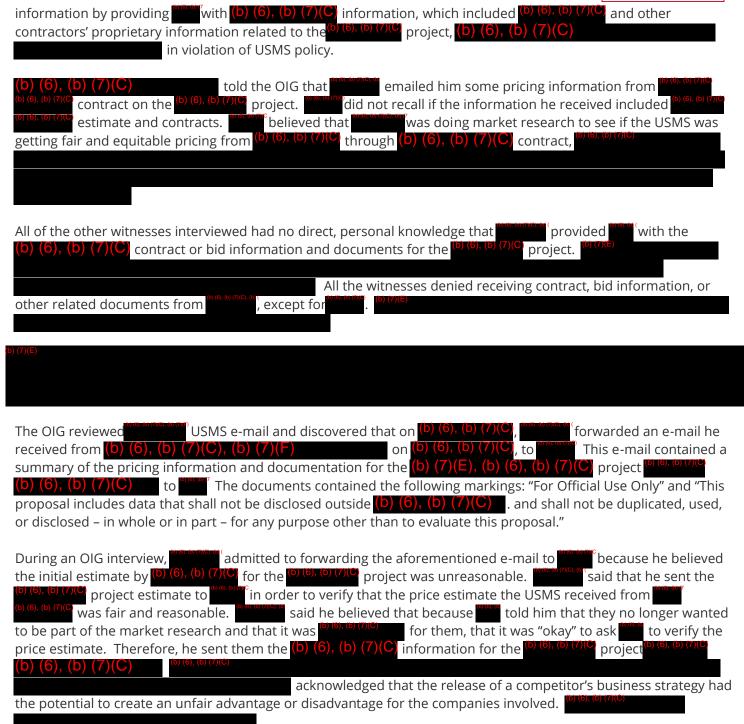


REPORT OF INVESTIGATION

SUBJECT					CASE NUMBER			
(b) (6), (b) (7)(C), (b) (7)(F)					(b) (6), (b) (7)(C)			
Acting Chief Deputy United States Marshal								
b) (6), (b) (7)(C)								
OFFICE CONDUCTING INVESTIGATION				DOJ COMPONENT				
Chicago Field Office				United States Marshal Service				
Chicago Ficia Office				States Marshar Service				
DISTRIBUTION			STATUS					
	Field Office	CFO	□ OPEN	☐ OPEN PENDING	G PROSECUTION			
	AIGINV		PREVIO	US REPORT SUBMITTED	:	⊠ NO		
×	Component	USMS		Date of Previous Report	:			
	USA							
	Other							
			S	YNOPSIS				
The De	partment of Ju	ustice (DOJ) (Office of the Inspecto	or General (OIG) initia	ated this investig	gation upon the receipt of		
informa	ation from the	United Stat	es General Services	Administration (GSA)	alleging that (b)	(6), (b) (7)(C) to		
(b) (6), (b)	(7)(C), United	States Mars	hals Service (USMS) /	Acting Chief Deputy	United States Ma	arshal ^{(b) (6), (b) (7)(c), (b) (7)(F)}		
(b) (6)	, (b) (7)(C)							
4								
(6) (6) (6) (7)(C)			6.					
(b) (6), (b) (7)(C								
During the course of the investigation, the OIG found indications that may have failed to safeguard								
_				and the same of th				
sensitive contract information by providing with (b) (6), (b) (7)(C) information related to the (b) (6), (b) (7)(C) project. The OIG investigation substantiated the allegation that (b) (b) (7)(C) information related to the (b) (b) (b) (7)(C)								
					.			
DATE January 11, 2021				(b) (6), (b) (7)(C)				
(b) (6), (b) (7)(C)			SIGNATU	SIGNATURE				
	BY SPECIAL AGEN	NT .			50			
DATE January 11, 2021			CICLIATIO	RE William	21	Digitally signed by WILLIAM		
William J. Hannah APPROVED BY SPECIAL AGENT IN CHARGE			SIGNATU	William	yourse-	Date: 2021.01.11 15:56:33 -06'00'		





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).

U.S. Department of Justice
Office of the Inspector General

PAGE: 2
CASE NUMBER: (0) (6)



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 United States Marshals Service (USMS) Acting Chief Deputy United States Marshal (b) (6), (b) (7)(C)

The OIG conducted this investigation jointly with the GSA OIG.

During the course of the investigation, the OIG found indications that way have also 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) information (7)

Investigation Process

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

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

Interviews of the following (5) (6), employees:



Interviews of the following GSA employees:



Review of the following:

- USMS e-mail
- training history

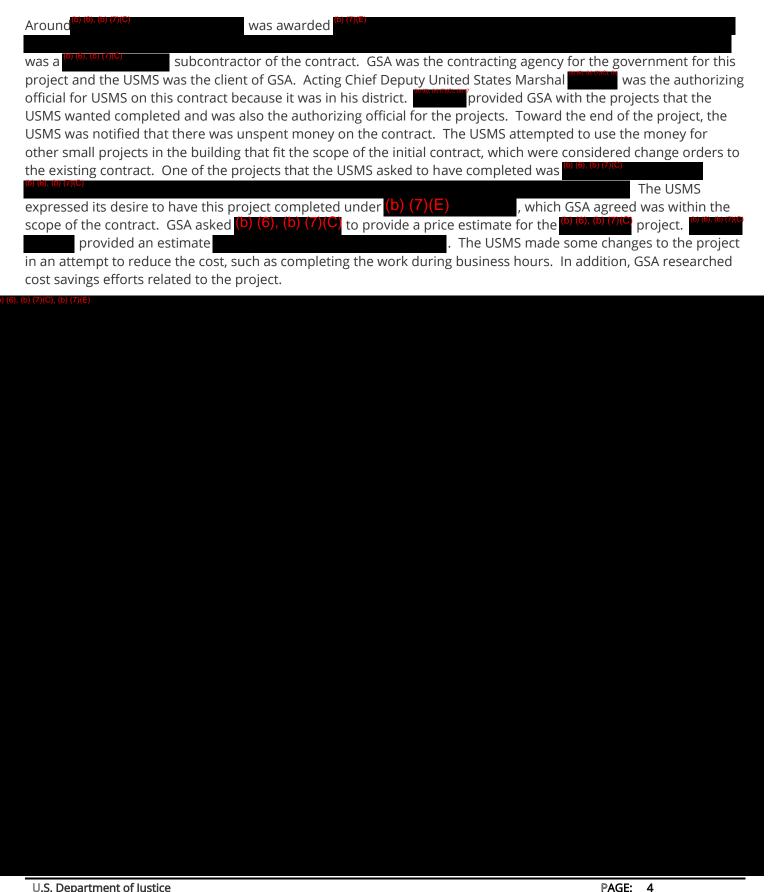
U.S. Department of Justice
Office of the Inspector General

PAGE: 3

CASE NUMBER:



Background



U.S. Department of Justice
Office of the Inspector General

CASE NUMBER: (b) (6).



(b) (6), (b) (7)(C), (b) (7)(E)	
U.S. Department of Justice	PAGE: 5

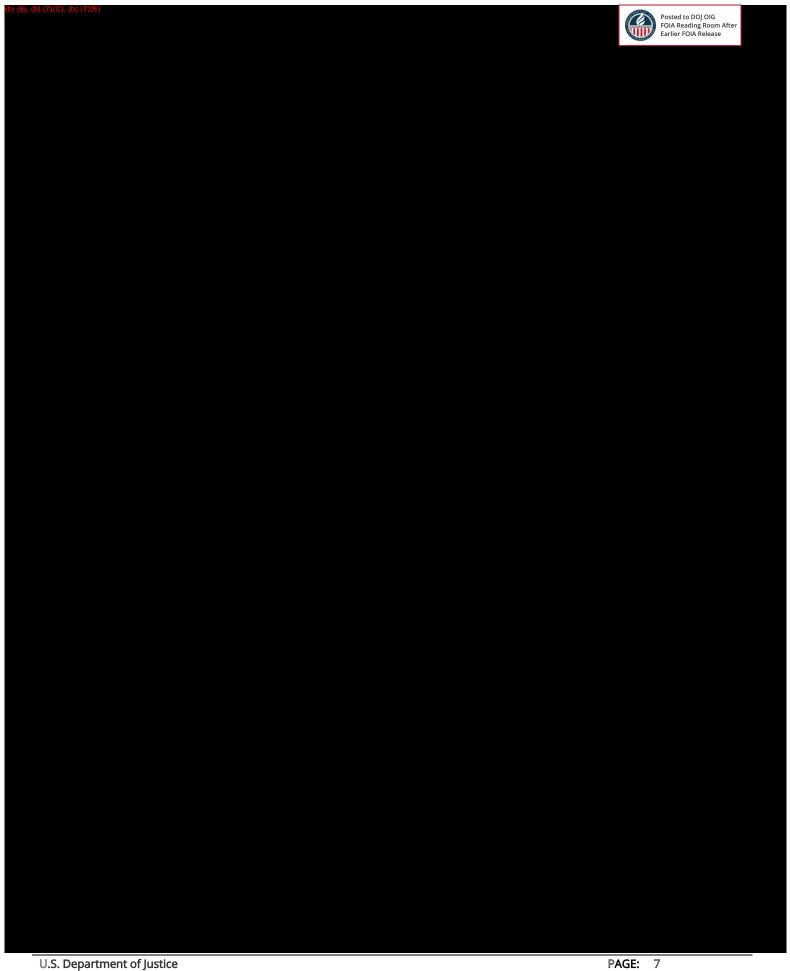
U.S. Department of Justice
Office of the Inspector General

CASE NUMBER: (6) (6), (b) (7)(C)



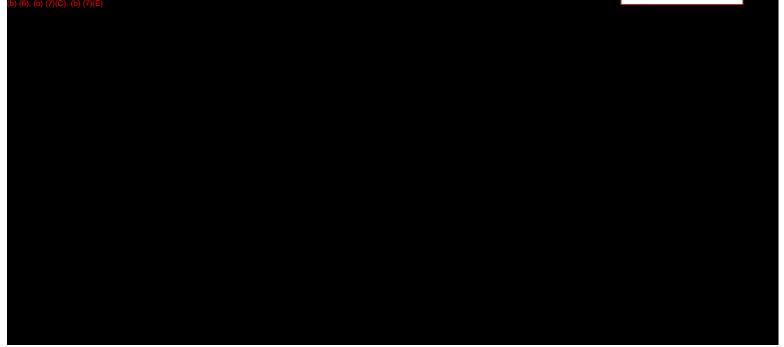
U.S. Department of Justice
Office of the Inspector General

PAGE:
CASE NUMBER:
DATE:
January 11, 2021



CASE NUMBER: (b) (6), (b) (7)(c)





Failure to Safeguard Sensitive Information

During the course of the investigation, the OIG found indications that 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)

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.

U.S. Department of Justice
Office of the Inspector General

PAGE:

CASE NUMBER:



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

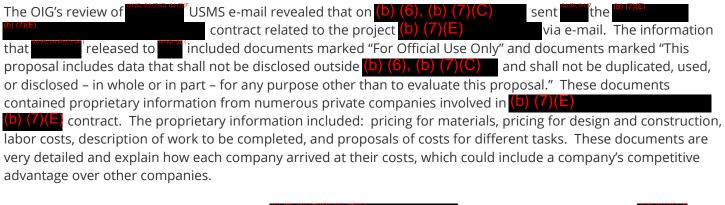
...

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 discussed USMS policy with USMS block of the violated USMS document security policy by providing another company's proprietary information to a potential competitor. believed that the USMS has the responsibility to honor a company/vendor's proprietary

U.S. Department of Justice
Office of the Inspector General

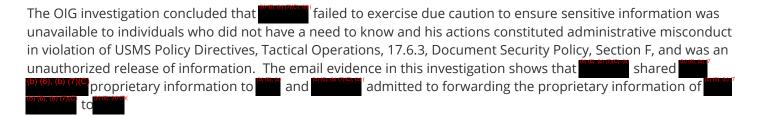
PAGE: 9

CASE NUMBER:



information and ensure it is not disclosed to a potential competitor. 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.

OIG's Conclusion



CASE NUMBER: (b) (6), (b) (7)(C)

PAGE: