



Defense Counterintelligence and Security Agency (DCSA)
DoD Insider Threat Management and Analysis Center (DITMAC)
Insider Threat Hotline
Request for Information (RFI)

This is a Request for Information (RFI) issued by the Defense Counterintelligence and Security Agency (DCSA). This RFI is issued solely for informational and planning purposes – it does not constitute a Request for Proposal (RFP) or a promise to issue a solicitation in the future. This RFI does not commit the Government to contract for any supply or service whatsoever. Further, DCSA is not at this time seeking proposals and will not accept unsolicited proposals. Responders are advised that the U.S. Government will not pay for any information or administrative costs incurred in response to this RFI; all costs associated with responding to this RFI will be solely at the responding party's expense. Not responding to this RFI does not preclude participation in any future solicitation, if any is issued.

The information and insights obtained under this RFI may be used in developing or refining existing procurement package documents and any eventual solicitation action(s).

Background

In December 2014, the Secretary of Defense appointed the DCSA to establish the Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) program; affirmed in January 2017 via DoD Directive 5205.16, Change 1. The mission of the DITMAC is to provide the DoD enterprise a capability to identify, assess and mitigate risk from insiders, to oversee and manage unauthorized disclosures, and to integrate, manage, mature and professionalize insider threat (InT) capabilities. DITMAC facilitates information sharing, collaboration, analysis, and risk mitigation across 43 separate DoD Components to address current and emerging threats to DoD personnel, assets, and information by insiders.

In 2022, the Secretary of Defense directed DITMAC to develop a DoD workforce InT hotline to create a department-wide virtual, anonymous reporting capability and triage management center. In support of this mission, DITMAC is seeking information related to a centralized hotline capability for the DoD workforce to report information on behaviors and/or actions that are indicative of a possible InT for espionage, sabotage, malicious cyber/network activity, suicide, or workplace violence. DITMAC will triage the InT hotline reports and refer them to the appropriate DoD Component InT programs via the InT case management system for validation and further analysis, if deemed necessary.

Overview of Requirements

DCSA has a potential requirement for a DITMAC Insider Threat Hotline solution, and is seeking information from vendors who are interested in and capable of performing the following:

- Meet and maintain Government compliance standards as listed in Attachment 1. Additional compliance standards not captured in the attachment may include internal DCSA policies, regulations and directives.
- Customize a commercial solution for the Government to receive and store hotline call, voice, and message data.
- Provide a secure public-facing web page that is able to receive, process and disseminate InT tips and provide guidance to users.
- Ability to timely and accurately triage reports and then route to the appropriate Component and/or point of contact.

- Document, archive, search, and retrieve all reports.
- Provide full access to perform audits of reports.
- Ability for unclassified reports to be submitted via telephone, email, instant messenger, text message, and website. Classified information will NOT be submitted via this solution; however, the website should provide instructions for users to submit classified tips through other means (i.e., SIPR e-mail address, JWICS).
- Provide voicemail-to-text capability allowing a caller to leave a voicemail that is then converted to text and/or report, and then submitted into the queue for review and routing.
- Provide a solution to address reports submitted during non-business hours.
- Provide a website with tailored questions relating to a specific type of incident where information can be submitted to provide additional details.
- Provide a standard operating procedure (SOP) for all InT hotline processes to be employed and keep a log documenting SOP version control through the life of the contract.
- Ability for all reporting domains to keep reporter anonymous.
- Provide technical support during all service hours. Core agency operating hours are 0800 – 1630 EST Monday through Friday, excluding Federal holidays.
- Aggregate and analyze metrics, reports, and response types.
- Ability to provide both routine and emergency system maintenance, patching, backup, and information updates.
- Consolidate all activity to a centralized dashboard infrastructure.
- Ability for the hotline solution to integrate with other DoD systems as necessary.

Proposed NAICS Code: The North American Industry Classification System (NAICS) Code 541512: Computer Systems Design Services (Size Standard: \$30M) is being proposed by DCSA. This industry comprises establishments primarily engaged in planning and designing computer systems that integrate computer hardware, software, and communication technologies .

The Government will consider other NAICS codes.

Requested Information

Interested vendors are requested to respond to this RFI by emailing Margaret Kroening at margaret.a.kroening.ctr@mail.mil, and Steven Chang at tzeleong.s.chang.civ@mail.mil. The response deadline is outlined on the associated SAM.gov posting.

Proprietary information and trade secrets, if any, must be clearly marked on all materials. All information received that is marked Proprietary will be handled accordingly. Please be advised that all submissions become Government property and will not be returned. All government and Contractor personnel reviewing RFI responses will have signed non-disclosure agreements and understand their responsibility for proper use and protection from unauthorized disclosure of proprietary information as described 41 USC 423. The Government shall not be held liable for any damages incurred if proprietary information is not properly identified.

Responses shall include the following information, at a minimum:

1. Entity Information
 - a) Vendor Name
 - b) Primary Point of Contact
 - c) Address
 - d) Phone Number
 - e) Unique Entity Identifier

- f) DUNS
- g) Point of Contact email
- h) Business Website

2. Business Type

Provide the economic business classifications you would potentially solicit under along with an updated capability sheet.

3. Contract Vehicles

Provide any contracting vehicles a future DCSA contract award may be placed against.

4. NAICS Code Recommendations

Provide either confirmation of the existing/recommended NAICS code as sufficient, or recommend an alternative NAICS code.

5. Requirements Response

Interested vendors are requested to provide white paper responses outlining possible technical solutions, capabilities, and cost/schedules, existing contracts where this service is available (e.g. GSA Schedule contract) related to the above mentioned requirements. Additionally, please indicate what previous contracts/orders has your firm performed like services under, along with any recommended best practices based upon previous work.

All correspondences should include the subject line: DCSA-RFI-DITMAC Hotline Services

6. Formatting

Please provide all responses in accordance with the page size and font indicated below. The cover page of the response shall include the company name, Unique Entity Identifier, DUNS Number, address, point of contact including phone number and email address, as well as the business size status of the responding company.

Page Size: 8 ½in X 11in, Microsoft Word (.docx) format

(11 X 14 inch or 11 X 17-inch foldouts shall count as two pages)

Font: Helvetica, Times New Roman, or Arial; no smaller than 14 point

7. Technical Processes and Solutions

- a. What commercial solutions do you utilize for initiating, maintaining, and sustaining hotline/call center services?
- b. The Government is focused on leveraging IT to the maximum extent possible to meet contract requirements. What IT solutions/processes are you currently using, or have you previously used, for automating hotline/call center services versus a typical manned call center?
- c. What processes do you utilize to categorize diverse data inputs (reports, inquiries, technical assistance) and sources (phone, email, text, messaging) to effectively distribute information?

- d. In addition to standard monthly and ad-hoc reporting, the Government requires the implementation and sustainment of a centralized dashboard. What solutions, both commercial and customized, are you currently using, or have you previously used to meet this requirement? Can the dashboard queries and data output be tailored by the various end users?
- e. As written, is your firm able to meet or exceed the listed requirements/desired capabilities within this RFI? Please indicate if there are any items which are:
 - Complex and time consuming to implement;
 - Not available commercially; and/or,
 - Costly to implement and maintain.
- f. Please provide any additional relevant information and/or advice for the Government to include within a future PWS to adequately capture commercial hotline best practices.

8. Vendor Teaming and Pricing

- a. Does your firm offer tiered pricing and corresponding levels of support/services? If so, please provide general information related to these different price levels and corresponding levels of service.
- b. What subcontracting or teaming, if any, do you foresee being necessary to perform this work? If teaming is anticipated, are these firms that you have previously worked with or have formal teaming arrangements in place with?

Industry Day: DCSA intends to hold an Industry Day prior to the closing of this RFI. The date and time will be provided in an addendum to this posting once finalized. The location will be virtual through a Zoom meeting. Link and instructions for joining will be provided to interested parties upon inquiry. Please reach out to Margaret Kroening at margaret.a.kroening.ctr@mail.mil to indicate interest in attending or ask any questions.

Vendor follow-on meetings: DCSA representatives may or may not choose to meet with interested Vendors. Such meetings would only be intended to have further meaningful exchanges of potential capabilities to meet the requirements.

Summary: This is a Request for Information only to identify sources that can provide the services pertaining to the subject requirement. The information provided in the RFI is subject to change and is not binding on the Government. DCSA has not made a commitment to procure any of the items discussed, and release of this RFI should not be construed as such a commitment or as authorization to incur costs for which reimbursement would be required or sought. All submissions become Government property and will not be returned.

ATTACHMENT 1
Applicable Publications

Listed below are publications that may be applicable to this potential future requirement.

Publication (Chapter/Page)	Date of Publication	Reference
Executive Orders		
Executive Order (EO) 10865	Issued: February 1960	Safeguarding Classified Information within Industry https://www.archives.gov/federal-register/codification/executive-order/10865.html
Executive Order (EO) 12829	Issued: 01/6/1993 Amended by Ex. Ord. No. 12885, and further amended by Ex. Ord. No. 13691, 2/20/2016	National Industrial Security Program https://www.archives.gov/files/isoo/policy-documents/eo-12829-with-eo-13691-amendments.pdf
Executive Order (EO) 12968	Issued: August 1995	Access to Classified Information https://www.govinfo.gov/content/pkg/FR-1995-08-07/pdf/95-19654.pdf
Executive Order (EO) 13764	Issued: January 2017	Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters https://www.govinfo.gov/content/pkg/FR-2017-01-23/pdf/2017-01623.pdf
Presidential Policy Directive (PPD) 19	Issuance Date: October 10, 2012	Protecting Whistleblowers with Access to Classified Information
Department of Defense Directives (DoDD): https://www.esd.whs.mil/Directives/issuances/dodd/		
DODD 5105.42	Issued: 08/03/2010 Change 1: 03/31/2011	National Industrial Security Program (NISP)
DODD 5205.16	Issued: 9/30/2014 Change 2: 8/28/2017	The DoD Insider Threat Program
DODD 5210.50	Issued: 9/30/2014 Change 2: 08/18/2020	Management of Serious Security Incidents Involving Classified Information
DODD 8140.01	Issued: 10/5/2020	Cyberspace Workforce Management
Department of Defense Instructions (DoDI): https://www.esd.whs.mil/Directives/issuances/dodi/		
DODI 1438.06	Issued: 1/16/2016 Change 1: 5/4/2020	DoD Workplace Violence Prevention and Response Policy
DODI 2000.16 (Volume 1)	Issued: 11/17/2016 Change 3: 5/7/2021	DoD Antiterrorism Program Implementation: DoD Antiterrorism Standards
DODI 5200.48	Issued: 3/6/2020	DoD Instruction – Controlled Unclassified Information (CUI)
DODI 5400.11	Issued: 1/29/2019 Change 1: 12/8/2020	DoD Privacy and Civil Liberties Programs
DODM 5200.01	Issued: 2/24/2012 Change Date: July 28, 2020	DoD Information Security Program: Protection of Classified Information (Vol 3 & 4)
DODM 5205.02-M	Issuance Date: November 3, 2008.	DoD Operations Security (OPSEC) Program Manual

	Change Date: October 29, 2020	
DODM 5220.22-M	Issuance Date: February 28, 2006. Change Date: May 18, 2016	National Industrial Security Program Operating Manual
DOD Financial Management Strategy	FY22-26 Version	https://www.comptroller.defense.gov/Portals/45/Documents/DoDFMStrategy/DoD_FM-Strategy.pdf