DoD Insider Threat Program

– Best Practices –

1.1 Hub Hiring

Rev 2

05/24/2017

The Under Secretary of Defense for Intelligence is the Senior Official for Insider Threat

Do you have any questions, comments, or concerns on this topic or others? Would you like to add your component to this Best Practices Edition?

If so, please contact the DoD Insider Threat Program at **osd.pentagon.ousd-intel.mbx.dod-insiderthreatprogram@mail.mil**

We look forward to updating and revising this edition, by adding other participants.

NOTE: The Best Practices series will deliberately be anonymized so that responses are not attributed to a participating Component with exception to the DoD Insider Threat Management Analysis Center (DITMAC), the Center for Development of Security Excellence (CDSE), and the National Insider Threat Task Force (NITTF). The information in this booklet is offered as guidance. It does not convey a task or directive. Each Component conforms to multiple and varying authorities. As such, each Component needs to confer with their Office of General Counsel (OGC) to verify their procedures conform to legal pronouncements.

Purpose:

The DoD Insider Threat Program has compiled data and information from several selected DoD Components that can offer field tested procedures which have produced credible results. These methods, techniques, and professional procedures are offered to Components to assist in their efforts to improve their respective Insider Threat Program (InTP). All best practices are informational, and individual programs should ensure any implementation actions are in compliance with their Office of General Counsel (OGC) and organizational policies before implementation.

Description:

This edition of Best Practices addresses questions pertaining to how Components have staffed the analysis positions embedded in the Hubs of their respective InTP. There are a total of 9 questions that were raised by Components which were then posed to 3 established Components.

Acronyms:

CI	Counterintelligence	**FY**	Fiscal Year	**OGC**	Office of General Counsel
CIO	Chief Information Officer	**GC**	General Counsel	**OUSD (I)**	Office of the Under Secretary of Defense for Intelligence
DSoS	DITMAC System of Systems	**HR**	Human Resources	**PBR**	Program Budget Review
DSS	Defense Security Service	**InT**	Insider Threat	**PM**	Program Manager
E-LMS	E-Learning Management Service	**IT**	Information Technology	**POM**	Program Objective Memorandum
EO	Equal Opportunity	**ITP**	Insider Threat Program	**PWS**	Performance Work Statement
FTE	Full Time Employee	**LE**	Law Enforcement	**SME**	Subject Matter Expert

Table of Contents

NOTE: Since DITMAC has a unique mission and is not a Component InT hub, some of these questions do not apply to them and they have been noted in those instances. Their responses still add value to the Best Practices series.

Q1. How did you staff your InTP Hub?

- *Did your Component Head or Senior Official establish new billets or redirect organic personnel billets to the program?*
- *Alternatively, has the Component Head or Senior Official levied "additional" InT duties onto staff personnel focused on other duties?*

DITMAC

In December 2014, when the Office of the Under Secretary of Defense for Intelligence (OUSD (I)) gave the incubation mission to Defense Security Service (DSS), the Deputy Secretary of Defense resourced us with 25 Full Time Employees (FTEs). The 25 FTEs all support the InT mission. Our sole mission is focused on InT and there are currently no additional duties.

Component #1

We redirected organic billets (cross discipline Law Enforcement (LE), Poly, Counterintelligence (CI), and Cyber). The component head has not levied additional InT duties onto hub staff.

Component #2

Our component redirected organic personnel and modified an existing contract to support the Hub. All Hub personnel have InT as their primary duty function. However, we do have several personnel from Human Resources (HR), Security, Information Technology (IT), Equal Opportunity (EO), General Counsel (GC) and CI that provide Subject Matter Expert (SME) support to the Hub as needed.

Q2. Have you gotten approval from the Component Head or Senior Official to add program personnel requirements (billets) into the Component's Program Objective Memorandum (POM)/budget?

- *Has your billet requests been endorsed/accepted?*

DITMAC

We were provided 25 FTEs. We will address emerging requirements in the Program Budget Review (PBR) Fiscal Year (FY) 19 process.

Component #1

To date, the answer is no. The program was limited to the programs provisioned in house. However, under the new InT Group Chief, requirements development is underway and will either be provisioned within the Agency, or programmed in the out years.

Component #2

Our component's ITP is captured as an "above-the-line" item in the budget beginning FY18. Currently, the program is funded utilizing reprogramed monies from the current component budget.

Q3. Was organizational guidance or policy established that governs or impacts the hiring of Hub analysts?

- *Was the guidance approved by the HR department and your supporting GC?*
- *Can you share the guidance you use with other Component Program Managers (PMs)?*

DITMAC

There was no specific guidance. Our component follows the DSS hiring guide that dictates all DSS hiring. We wrote specific position descriptions for each of our billets. We will share the position descriptions as well as of our contract Performance Work Statement (PWS) for the SMEs.

Component #1

No, there was no guidance or policy established that governs or impacts the hiring of Hub personnel.

Component #2

Our component's ITP is currently staffed with one civil servant (GG-15-0132) and four (4) contract personnel. Our component is not scheduled to add additional civilian billets to the program until FY18/19.

Q4. What personnel roles/titles serves within your Hub?

- *Besides analysts, do you have engineers, psychologists, IT specialist, etc., that play a role in the Hub?*
- *Are there any personnel that play a unique role or more than one?*

DITMAC

We have branch chiefs (GG-14) that serve in a SIA/SIO type capacity and InT analysts (GG-9 through GG-13). We also have contractor SMEs; to include a Behavioral Advisor and a Senior CI/LE Advisor on staff currently. This year we will be adding a Cyber Specialist and HR expert to our SME panel.

Component #1

Yes. We have Detection Analysts, Engineers, Data Base Specialists, IT Specialists, Psychologists (reach back to unit, not in house), and Case Management Specialists.

Within the Insider Threat Group (ITG), there are 3 Senior Deputies representing CI, Security and Chief Information Officer (CIO). Each of these Deputies lead their specific discipline and form a core leadership team under the Chief of the overall ITP. In this capacity, they cover all functional areas.

Component #2

All personnel in the Hub are either analysts or IT specialists. We are exploring the possibility of adding a psychologist to the program in FY18. No personnel has an unique role or more than one within our Hub.

Q5. Are the personnel assigned to the program confined to a specific occupational series (e.g. 0080; 0086; 0132) or does occupational specialty impact personnel utilization in the program?

- *Do you use a written and aligned a position description to each position operating within your Hub?*

DITMAC

Our InT analysts are in the 1801 or 0132 occupational series. We've tried to strike a balance between the two. Occupational specialty definitely matters when being assigned to the Hub. That is why we have included two series to ensure we are balancing the right capabilities and talents. We do not directly handle or receive any cyber related data. That is why we do not have that series included. We do recognize the importance of cyber knowledge and we will have a contract SME on staff in the near future.

Component #1

We use 0132, 2210 and 1800 series. For Detection Analysts, there is a written and aligned position description.

Component #2

Currently the ITP is staffed with one (1) GG-15-0132. We are however concerned with the possibility of E.O 12333 having a negative impact on the program. We have worked with our GC to isolate the program and the duties of the individual. We have also explored the possibility of changing the individual job series and are hoping that the Under Secretary of Defense for Intelligence (USD (I)) or the Office of Personnel Management (OPM) will provide guidance on how to best proceed. We have a position description for our ITP Manager.

Q6. Do you use DoD contractors within your Hub?

- *What limitations, if any, have you levied on their duties or functions?*
- *What is the approximate ratio between contractors and staff and is there significance behind this ratio?*

DITMAC

Yes, we do leverage contractors. We have used them to support larger supporting efforts like DITMAC System of Systems (DSoS) and risk model development. However, those contractors will only support the DITMAC through the development of those capabilities so they are more short term in nature. In addition, we have contractors that are more embedded in day to day DITMAC activities. Our SMEs are all contractors. The SMEs are there to provide advice and counsel. We have 2 on staff and plan to bring on 2 more this FY. We also have a contract paralegal. We will also be adding some contracted InT analysts to the staff this year. There are 4 planned for this year with 2 possibly being added next FY. There are 17 total FTEs in operations including 1 Assistant Director (GG-15), 1 Deputy Assistant Director (GG-14 non-Supv), 3 Branch Chiefs (GG-14 Supv), and 12 analysts (GG-9-GG13). There is no formula that drives the ratio of government versus contractor. DITMAC is capped at 25 FTEs, so we have to supplement with contractor staff. For the SMEs, in order to get personnel with the required level of expertise we had to leverage contractors.

Component #1

Yes, our component utilizes contractors and there are all required to sign a Non-Disclosure Agreement (NDA). We also monitor their use of the sensitive InT based systems. The ratio between contractors and staff is 1-1; 50% of the workforce are contractors, there is no significance.

Component #2

Yes we do. We currently do not limit our contractors on the information they can review. However, all decisions as to whether we open, close, or refer an incident, are the sole duty and responsibility of government personnel. Our current staffing is one (1) civil servant to four (4) contractors.

Q7. Since Hub personnel have access to sensitive personnel information, do you require your that they sign a NDA that restricts or limits the pool of authorized recipients?

- *Has your supporting GC approved the form and this practice?*

DITMAC

Yes, all of our Hub staff signs NDAs which were approved by the DSS GC.

Component #1

Yes, all Hub personnel are required to sign a NDA and our GC has approved this practice. However, the form that we have been using has not been approved by GC and is currently being reworked.

Component #2

Yes, all Hub personnel, as well as personnel that supports the program, are required to sign a program-specific NDA and attend annual security training. Our GC assisted in the development of our NDA and fully supports the practice of using it for all personnel supporting the program.

Q8. During the course of an 8-hour work day (40-hour work week), are your Hub analysts working solely on InT duties?

- *Are they dual-hatted or working other duties not aligned with InT Hub functions?*
- *If they are dual-hatted, how have you arranged to have a functional analysis capability?*

DITMAC

Yes. Due to the unique mission of the DITMAC, compared to the DoD Component InT Hubs, our InT analysts only work InT issues and are not dual-hatted.

Component #1

Yes, all Hub personnel work solely on InT duties. No personnel in the hub are dual-hatted.

Component #2

Yes, all Hub personnel work solely on InT duties and none are dual-hatted.

Q9. Have you implemented standardized training and/or professional development for analysts working in the Hub?

- *Is it documented?*
- *Can you share this with other Component PMs?*

DITMAC

Yes, we have an InT Analyst training matrix that spans training on traditional analysis, writing and briefing skills, as well as training across the InT pillars including CI, Security, Cyber, HR, etc. We have also identified a few privacy related courses. All of our analysts are required to attend the NITTF Hub training as well.

Yes, we are happy to share. We shared our training matrix with CDSE and others.

Component #1

Informally, all personnel have taken the National Insider Threat Task Force (NITTF) training and approximately 50% have taken the trigger development training. There is an effort underway to formalize a training program for all InT Staff, but as of now, nothing is documented.

Component #2

Informally, in addition we conduct training twice a year for all personnel that work in the Hub and/or support the program.

Yes, all training is capture in the E-Learning Management System (E-LMS). In the past we have made our training available to others if requested.

Q10. Where can Component InTPs find the position descriptions and standardized trainings aforementioned in this document and noted as available to DoD PMs?

OUSD (I)

If you are interested in any positions descriptions or standardized trainings that were listed as available to PMs, please contact the DoD Insider Threat Program. Participating components are willing to share if you reach out to them directly. The DoD Insider Threat Program will provide you with the proper point of contact for the information you seek.