# Demystifying Operations Security (OPSEC) Assessments: A “How To” Primer

## ***OPSEC Assessments Purpose: Determine susceptibility to adversary exploitation***

Operations Security (OPSEC) is commonly defined as the process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning operations or other activities (“Loose Lips Sink Ships”). Integral to the OPSEC process is the requirement to conduct regular OPSEC Assessments. The Department of Defense Directive (DoDD) 5205.02, Operations Security, dated 06 March 2006, defines an OPSEC Assessment as “An evaluative process, usually conducted annually, of an operation, activity, exercise, or support function to determine the likelihood that critical information can be protected from the adversary’s intelligence.” Additionally, Joint Pub 3-13.3, Operations Security, dated 29 June 2006, describes an OPSEC assessment as “an intensive application of the OPSEC process to an existing operation or activity by a multi-disciplined team of experts. Assessments are essential for identifying requirements for additional OPSEC measures and for making necessary changes in existing OPSEC measures.”

Assessments are conducted only after an organization has identified its Critical Information (CI). Critical information is defined as “Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequence for friendly mission accomplishment (Joint Pub 1-02). CI is often referred to a subset of Essential Elements of Friendly Information (EEFI). For example, an EEFI would be “When will the special operation commence?” and the corresponding CI would be “Saturday, January 6th, 0600.” The identification of CI is important in that it focuses the OPSEC Assessment on evaluating protection of vital information rather than attempting to protect all classified or sensitive information. The list below serves as a good reference to generate a CI list for your organization:

- UNIT CAPABILITIES OR DEGRADATION
- DETAILS OF PLANS, OPERATIONS, ORDERS, OR PROGRAMS
- REFERENCE OF MISSION ASSOCIATED INFORMATION, SUCH AS PERSONNEL/EQUIPMENT DEPLOYMENT DATES OR LOCATIONS
- SPECIFIC TAD/TDY DEPLOYMENT DATA, INCLUDING PERSONNEL NUMBERS, DURATION, LOCATION, SYSTEMS, ETC.
- SPECIFIC DETAILS CONCERNING TAD/TDY TRAVEL ITINERARIES AND PURPOSES OF TRAVEL BY KEY PERSONNEL
- ASSOCIATION OF ABBREVIATIONS, ACRONYMS, NICKNAMES, OR CODEWORDS WITH PROJECTS OR LOCATIONS
- NEW, PROJECTED, OR EXPANDED SECURE COMMUNICATIONS CAPABILITIES

OPSEC assessments are different from security evaluations or inspections in that an assessment attempts to reproduce an adversary’s view of the operation or activity being assessed. Independently, a security inspection seeks to determine if an organization is in compliance with the appropriate security directives and regulations. Essentially, OPSEC assessments enable an evaluation of current OPSEC measure effectiveness.

Although OPSEC Assessment findings are not provided to the assessed unit's higher headquarters, Commanders or OPSEC assessment teams may forward to senior officials generic lessons-learned on a non-attribution basis. Lessons-learned from assessments should be shared with command personnel in order to advance the command's OPSEC posture and mission effectiveness. Further, leaders and decision makers are shown the resources required to adequately protect against adversary exploitation. Findings should be labeled and handled at appropriate classification level (SECRET or CONFIDENTIAL) depending upon vulnerability results. See your Information Security Manager for guidance. COMFLTFORCOM states in 042111Z Jun 04 message that, "Leaders must pursue every effort to ensure that highest OPSEC measures are followed and OPSEC integrity is maintained. Make OPSECC a priority with daily emphasis from senior command personnel to the newest requite and observe strict adherence to OPSEC in all transactions and/or communication lines to ensure classified or otherwise sensitive information is not inadvertently disclosed."

OPSEC Assessment bottom line: OPSEC is emphasized, security is improved, threat awareness raised and mission success rate increased. Of note: "Operations Security" is not the same as "Operational Security." The former focuses on protecting unclassified indicators to critical information from the adversary's perspective while the latter, although not defined in Joint Pub 1-02, is commonly associated with physical protection measures regarding building or network access concerns.

## Recommended assessment procedures

The steps listed below provide the basic and logical steps to conduct an OPSEC Assessment and have been used at many Department of Defense (DoD) shore based, Navy ships and forward deployed organizations world wide with consistent, positive results. It is highly recommended that all the steps be read first to gain insight to the entire assessment process prior to its execution. For example, if communications security (COMSEC) monitoring is going to be part of the assessment, scheduling may take several months. Although no specific or unique training is required to administer and conduct an OPSEC assessment, it is assumed that the organization's OPSEC Officer and working group members have completed basic OPSEC education and understand OPSEC fundamentals. If training is required, OPSEC training sources (formal and CBT) are referenced at the very end of this document. Complete each step in the order listed below:

### Steps:

1. Complete the "Rate Your OPSEC" survey below to determine the status of your organization's OPSEC program. Upon completion, proceed to step 2.

### Rate Your OPSEC Instructions:

**Assess your command's OPSEC posture by completing the following questions.**
**Insert 10 for a "Yes" response, 0 for a "No" response and 1-9 in "Progressing" (depending on the degree you feel your command is at in regards to that question.)**

| | YES | NO | Progressing |
|---|---|---|---|
| **1. Does your command have an OPSEC Officer in writing?** | 🟩 | 🟥 | ▨ |

| | | | | |
|---|---|---|---|---|
| 2. Has the OPSEC Officer received formal OPSEC training or completed the OPSEC 1301 CBT? | | 🟩 | 🟥 | ▨ |
| 3. Does your command have an OPSEC instruction? | | 🟩 | 🟥 | ▨ |
| 4. Has your command conducted an annual OPSEC assessment? | | 🟩 | 🟥 | ▨ |
| 5. Does your command have an OPSEC working group? | | 🟩 | 🟥 | ▨ |
| 6. Is your command's Critical Information available to all personnel for awareness? | | 🟩 | 🟥 | ▨ |
| 7. Does the command have a shred or paper destruction Policy? | | 🟩 | 🟥 | ▨ |
| 8. Does the command provide OPSEC training during command indoctrination? | | 🟩 | 🟥 | ▨ |
| 9. As a minimum, does the command provide yearly OPSEC GMT? | | 🟩 | 🟥 | ▨ |
| 10. Does your command utilize OPSEC awareness products? (I.E. Posters, signs, etc.) | | 🟩 | 🟥 | ▨ |
| | Total score = | **0** | | |

**Upon score calculation, determine whether your program is satisfactory or requires improvement. Scores greater than 85 represent OPSEC programs that require minor adjustments. Scores less than 85 require greater emphasis and concerns should be addressed immediately.**

**2.** In the event you answered “No” to the Rate your OPSEC survey questions: (1), (2), (3), (5), or (6), then corrective action needs to be taken prior to conducting an assessment. When the survey answers are “Yes” or found to be satisfactory, proceed to step 3.

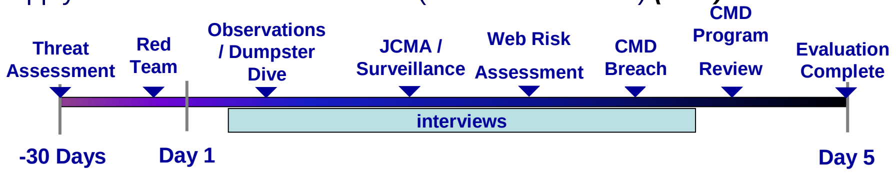
**3.** Assemble your Working Group to determine an appropriate execution timeline for this assessment. To optimize the effectiveness of an OPSEC program or assessment, a comprehensive understanding of relevant processes, activities, business practices, and applicable critical information is required. This is most easily obtained through a working group whose representatives (at least one) are derived from each division, department, directorate, etc. For example, Operations, Communications, Logistics, Intelligence, Administration, Public Affairs, etc. each should include a participating team member. Another benefit is that the working group will consist of subject matter experts with intimate knowledge of routines, inter-workings, and potential vulnerabilities. If involved with Information Operations (IO) missions or planning, including Psychological Operations (PYSOP) and Military Deception (MILDEC) representatives will improve the OPSEC working group's impact to mission success. If not already completed, the working group will generate the Critical Information list. It is recommended the events proceed in the following order to include, but not restricted to: (details of each broken out farther below)

A. In Brief
B. Threat brief
C. Red Team activities
D. Observations, space walk-throughs and dumpster dives
E. Conduct OPSEC interviews
F. COMSEC Monitoring
G. Web Risk Assessment (WRA)
H. Physical and electronic integrity breach
J. Command program review
K. Assessment wrap-up; Plan of Action & Milestones (POA&M)

Below is a generic timeline depicting the general sequence of events:

## Timeline

- Verify CI / EEFI ***(Date)***
- Obtain threat assessment: NCIS ***(Date)***
  - – Foreign intelligence service collectors, terrorists, criminals
- Identify Vulnerabilities / Conduct assessment ***(Date)***
  - – Evaluate command emphasis, awareness, training; conduct interviews
  - – Emulate threat: Open source discovery, dumpster dives [*test physical security, observe routines, monitor comms & network – not performed*]
- Assess risk of vulnerability findings ***(Date)***
- Apply / evaluate countermeasures (recommendations) ***(Date)***



Sample five-day assessment daily POA&M:

### Monday (Day Month Year)

| | |
|---|---|
| 0900 | Team leaders muster |
| 0930 – 1415 | Surveillance of building(s); Dumpster dives; Working Group members walk through assigned spaces with checklist |
| 1430 | Team leaders muster for debrief |

### Tuesday (Day Month Year)

| | |
|---|---|
| 0900 | Team leaders muster |

| | |
|---|---|
| 0930 – 1415 | Surveillance / intrusion of building(s); Conduct interviews / space walk through |
| 1430 | Team leaders muster for debrief |

### Wednesday (Day Month Year)

| | |
|---|---|
| 0900 | Team leaders muster |
| 0930 – 1415 | Intrusion of buildings; Dumpster dives; Policy review; Conduct interviews / space walk through (cont.) |
| 1430 | Team leaders muster for debrief |

### Thursday (Day Month Year)

| | |
|---|---|
| 0900 | Team leaders muster |
| 0930 – 1415 | Intrusion team compile findings for out brief; Policy review (cont.) / compile findings for out brief<br>Conduct interviews / space walk through (cont.) |
| 1430 | Team leaders muster for debrief |

### Friday (Day Month Year)

| | |
|---|---|
| 0900 | Team leaders muster |
| 0930 – 1215 | Conduct interviews / space walk through (cont.) / compile findings for out brief<br>Dumpster dives / compile findings for out brief |
| 1300 | Final Out Brief (all WG members) |

A. Threat brief

Commander, NETWARCOM recently commented on the persistence of adversarial intent and capability: “The threat vector is 360 degrees, the enemy is ever vigilant probing and collecting 24/7, and our information is constantly at risk, at work and at home. You must be at GQ round the clock.” In order to understand what threats are relevant to your organization, obtain a local threat briefing from the organization’s intelligence representative or Service investigative branch agent (i.e. Navy would contact the Naval Criminal Investigative Service [NCIS]). The presentation will provide actual adversarial intentions and capabilities that need to be emulated in support of the assessment. This brief should be presented prior to the execution phase of the assessment, as it will raise the level of awareness of all personnel. Without this brief, an assessment may focus on erroneous adversary capabilities and portray irrelevant vulnerabilities.

B. Red Team activities

A group of individuals with proper authorities will replicate adversary capabilities as outlined in the Threat Brief. By simulating malevolent intent via a wide spectrum of institutional or ad hoc methodologies, potential vulnerabilities are usually uncovered. From network penetration to dumpster dives and from attempts to gain building access without proper identification to monitoring conversations at local areas of personnel congregation, the Red Team demonstrates the adversary’s view. After weaknesses are identified, specific mitigation strategies are developed to prevent exploitation. Before the assessment begins, Red Team members and activities will be identified and approved via a document (otherwise known as a “Get out of Jail free Card”) by the organization’s Commander, OPSEC and Security Officers.

C. Observations, space walk-throughs and dumpster dives

These functions can be conducted by working group members or the Red Team. Through observations, one can identify potential vulnerabilities via visible indicators, predictable patterns, entrance procedures, poor security practices, etc. Dumpster-dives reveal the organization’s policy on discarding documentation, classified and unclassified. Team members will explore discarded contents in workspace and outside containers for disclosures of the organization’s critical information (operation or exercise). Even though an organization may not “own” the dumpster at the end of the pier, it is imperative to identify what an adversary will have access. Immediately inform the information security officer / manager once classified information is discovered. Policy changes are typically recommended upon assessment observation and dumpster dive findings. Use the following list to conduct a space walkthrough. Comment on any poor security practices noticed during walk-through not listed below:

Office/Space checked: _____________ Date checked: __________

_____ CI Cue Card (Yellow Card) posted near phone/computer?
_____ Posters Posted
_____ Phone stickers on phones and legible
_____ Shredders available and operable
_____ Burnbags available
_____ Personal information in the open/posted
_____ Unoccupied computers logged on
_____ Computer passwords written in open
_____ Computer screens facing windows
_____ Safes locked when not is use
_____ Cell phones in spaces

Use the following checklist for trash searches:

Trash / Recycle Receptacles or Dumpster location ________ Date / time checked: __________

____ Privacy Act information, to include but not limited to SSN, addresses, phone numbers, and family information
____ POD / POW
____ Documents related to command, mission and critical information
____ Supply requests and / or equipment inventories
____ Discarded / unopened mail, whether personal or command specific
____ Itineraries / VIP schedules
____ Joint/ Navy doctrine, publications and instructions

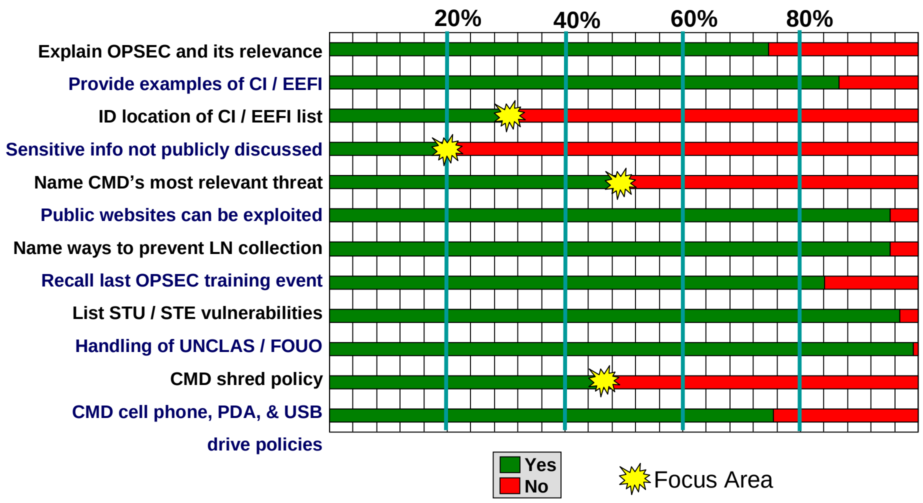
D. Conduct OPSEC interviews

OPSEC interviews provide a non-attributable means of acquiring insight to potential vulnerabilities that organizational personnel may be aware of, yet tend not to disclose during the course of everyday activities. The names of the interviewees are NOT disclosed to facilitate non-attribution. Questions are developed by the OPSEC working group to gain insight to OPSEC awareness and practices. Often the questions reflect the chief concerns of the Commander. Responses are collated and integrated into the out brief. It is recommended that working group members pair-up and interview organizational personnel, preferably not from the interviewer's division, department, etc. Interviewers from different areas of the organization tend to make those interviewed more comfortable and able to provide honest answers, not the answers they think the organization wants to hear. Optimally, one-person interviews an individual while another records the response. However, other interview options may be used to attain the required insight to the OPSEC posture. For example, one can interview small groups of similar ranking personnel, similar division personnel, etc. Sample interview questions

Regarding the number of interviews required: depending upon the organization's size, number of interviewers and time allotted, the working group will propose – the commander decides – on a "representative sample" percentage. As with any survey / polling data, the smaller the sample size, the less accurate the results. Ten (10) percent is usually too small and one hundred (100) percent is often too difficult. If each working group member interviews seventy (70) percent of each division, then a representative sample is readily achieved. As personnel are the key to protecting an organization's critical information, OPSEC interviews are fundamental in understanding their ability to prevent its exploitation.

Metrics from interviews are focus-area indicators. Keep the number of questions to ten or twelve. Ask open-ended questions, but grade them as "yes" or "no." Therefore, data from hundreds of interviews can be simply captured in spreadsheet form. For example, ask, "Explain what OPSEC is and why it is important." Correct responses will be marked "yes" and incorrect responses marked "no, "as the following slide depicts:

**Combined Total (126)**



E. COMSEC Monitoring

Unfortunately, personnel commonly discuss an organization's critical information via un-secure government communications (phones, email, etc.). Army

General McKiernan stated in August 2006 that, “Even when the user turns it off, a wireless device can be remotely turned on to eaves drop and retransmit conversations, typically within 20 feet of the device. Because there are no external indications of active use, the user will not know that the device has been turned on.” If requested, your organization can request and authorize the Joint COMSEC Monitoring Activity (JCMA) monitor government communications for references of the organization’s critical information (working group provides target information to JCMA). Prior to communications monitoring, it is imperative that personnel are provided notice of proposed monitoring (attain Legal Council approval). Results are typically compiled daily and provided to a single designated individual (i.e. OPSEC Officer). Findings identify whether or not personnel divulge critical information via un-secure communications modes and are non-attributable as the offender’s name is not identified, only the revealing disclosure content.

F. Web Risk Assessment (WRA)

An Al Qaeda training manual recovered in Afghanistan states, “Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of information about the enemy.” Justifiably, information posted on an organization’s publicly accessible website must be regularly reviewed to ensure it is free of critical information and or information that provide adversarial advantage. Additionally, web site material will be analyzed for accumulation of seemingly unrelated topics that when aggregated, disclose information useful to adversaries. SECDEF promoted in an Information Security/Website Alert on August 2006, “All personnel have the responsibility to ensure that no information that might place our service members in jeopardy or that would be of use to our adversaries is posted to websites that are readily accessible by the public.”

During an assessment, a working group or Red Team member will review the organization’s web page for Critical Information as well as ensure compliance with DoD regulations and instructions. The Navy Information Operations Command Norfolk maintains a cadre of Web Risk Assessment experts and a website (https://www.nioc-norfolk@navy.mil/operations/wra/wra.shtml) filled with resources (checklists, references, etc.) promoting effective WRA. Findings must be discussed with the Public Affairs Officer.

G. Physical and electronic integrity breach

If applicable, approved and pre-coordinated, Red Team personnel will attempt to compromise building integrity through attempts to bypass or circumvent physical and / or electronic security measures. The Red Team should never cause physical damage to any property or person while conducting their duties as a simulated aggressor. It is, however, acceptable to leave a mark, i.e. Red Team sticker, to illustrate the fact that vulnerability was identified and the potential of compromise or disclosure was probable. Before the assessment begins, Red Team members and activities will be identified and listed on a limited distributed document (Get out of Jail free Card). The following checklist serves as a good reference:

_____ Badges properly checked at Entrance / Quarterdeck
_____ Badges openly worn outside
_____ CO/XO or VIP arrival/departures repetitive
_____ Building doors secure during / after hours
_____ Outside exit only doors secured

_____ Cipher locks easily bypassed
_____ Piggybacking occurs (someone holds door, others enter without swiping badge)
_____ Shoulder Surfing opportunities exit (ease of observing other's PC screens)

Date of intrusion attempt: __________ Building: __________ Areas observed / Areas breeched: _____________

H. Command program review

During this portion of the assessment, a designated team member from the working group should review all applicable documentation and procedures related to the organization's OPSEC program. For example, has the OPSEC Officer and working group members obtained current letters of designation? Has training been conducted and documented? Have instructions and standard operating procedures (SOPs) been updated? Use the checklist below to gauge the adequacy of your program:

____ OPSEC Officer designated via appointment letter
____ Critical Information List (CIL) developed, relevant and posted near PCs, phones, copiers, faxes, shredders, etc.
____ Assessment results from previous year (formal and/or informal)
____ Command OPSEC instruction, policy, or plan on file
____ Personal Electronic Device (PED) policy
____ Shred policy

I. Assessment wrap-up; Plan of Action & Milestones (POA&M)

When all assessment activities are complete and data compiled for summarization, it is recommended that a Power Point brief be built for the Commander's out brief. The out brief should include key findings and recommendations for corrective action with specific remediation milestones and designated action officers. This brief should serve as a POA&M template for the working group to identify and track all deficiencies and prepare them for the six-month follow-up report.

**4.** Based on the above, present Commanding Officer with an In-Brief prior to the assessment and obtain approval to proceed. Proceed to step 5.

**5.** Request COMSEC monitoring support if required / needed. Due to many requests for this limited resource service, scheduling must be done months in advance. If this resource is not available, continue with the assessment but make a note of it during the Out-brief. Proceed to step 6.

**6.** Contact command Intelligence department, (i.e. N2, G2, S2, J2 etc.) or Service investigative branch (i.e. NCIS, OSI, CID, etc.) for a threat brief / analysis of local threat intent and capabilities. Proceed to step 7.

7. Assign team leads for designated portions of the assessment (i.e. Dumpster dive, Interviews, Observations, etc.). Proceed to step 8.

8. Begin assessment in accordance with your POA&M. After each assessment activity has been executed, proceed to step 9.

9. Upon completion of the execution phase, and all information has been gathered, it is recommended the working group begin compiling a comprehensive report to present findings to the Commander. It is recommended a short Power Point brief reflecting these findings and recommendations for corrective action are presented to the Commander.

SECDEF's DODDIR 5205.02 directs, "As an operations activity, OPSEC will be considered during the entire lifecycle of military operations or activities" and "Ensure adequate practices are in place to prevent adversaries from taking advantage of and aggregating publicly available information...and other detectable activities to derive indicators of U.S. intentions, capabilities operations and activities." Conducting OPSEC assessment via the steps outlined above ensures SECDEF requirement fulfillment.

Sources for OPSEC training are available at the following websites:

| | |
|---|---|
| IOSS | http://www.ioss.gov |
| JIOC | http://josc.jioc.smil.mil (SIPR only) |
| Army | https://www.1stiocmd.army.mil/io_portal/Public/Pages/Pulic_main.cfm |
| Navy / USMC | https://www.nioc-norfolk.navy.mil/operations/opsec |
| Air Force | https://www.afiwcmil.lackland.af.mil.opsec/index.cfm |

***Check out ***wiki-pedia's*** definition of OPSEC. Search ***wiki-how's*** "How to Conduct an OPSEC Assessment." ***

For more information regarding OPSEC assessments or to obtain OPSEC assistance, contact the Navy OPSEC Support Team (NOST) at opsec@navy.mil or visit the web page at www.nioc-norfolk.navy.mil or www.nioc-norfolk.navy.smil.mil.

*Article submitted by LCDR Daryl Haegley, Navy OPSEC Support Team OIC and NETWARCOM's Force OPSEC Program Manager located at Navy Information Operations Command-Norfolk. Winner of National OPSEC Individual Achievement Award and DOD CIO Award, he is an Operations Security Certified Professional (OCP).*

# ARTICLE #2

## Navy Multi-Discipline Vulnerability Assessment (N-MDVA) Program

***N-MDVA Purpose: Strengthen Naval Forces' warfighting effectiveness as N-MDVA enhances a Commander's ability to identify and improve the command's overall IO readiness***

NIOC-Norfolk has initiated a Navy Multi-Discipline Vulnerability Assessment (N-MDVA) program. The purpose is to provide a standardized, full-spectrum Information Operations (IO) assessment capability to evaluate Naval Forces' ability to defend against adversary IO and provide specific actionable remediation, certification, and training recommendations. As the N-MDVA program matures and acquires additional resources, the N-MVDA team currently focuses on two of the five core IO capabilities: Computer Network Operations (CNO) and Operations Security (OPSEC). In the not too distant future, N-MDVA's will encompass the three other IO capabilities (Military Deception, Electronic Warfare and Psychological Operations) facilitating realization of a full-spectrum IO assessment capability.

The N-MDVA program expects to assess Strike Group packages entering the Basic Phase of the pre-deployment portion of a Fleet Response Training Plan (FRTP) cycle, at an initial rate of approximately three per year and one shore command per year. Ad-hoc assessments for requesting Commands will be considered if N-MDVA resources and operational schedules permit.

N-MDVA is conducted by teams of specialists trained, with proper authorities, to identify exploitable information and information systems using the full spectrum of IO assessment activities. The team's focus is on identifying vulnerabilities, assessing risks, and developing a plan with the assessed organizations, to reduce unacceptable risk. The team's expertise facilitates identification of best practices and other measures designed to reduce vulnerabilities based on the organizations environment, threats, and resources. N-MDVA teams may remain engaged with a customer organization to assist with training or implementation of approved countermeasures, or until further assistance is no longer required.

Activities that may be included in an N-MDVA assessment:

-OPSEC Program Review
-Open Source collection (publicly available information)
-Network Vulnerability Assessment
-Web Risk Assessment
-Network Penetration
-OPSEC Interviews
-Communications Security (COMSEC) monitoring
-Telecommunications (TELECOMM) Monitoring
-Radio Frequency (FR) Monitoring
-Surveillance / observation
-Physical Security Assessment
-Human Vector Analysis (HVA)

-Trash Intelligence / Dumpster Diving

Assessments are synchronized and coordinated with existing organizational capabilities, typically following the same procedural format as traditional OPSEC assessments (outlined in OPNAVINST 3432.1 and Joint Pub 3-13). N-MDVA teams can be employed as an OPFOR capability to train forces against a realistic IO threat with goals of improving readiness, validating TTPs, employing IO related methodologies, and conducting other activities that require a credible IO adversary.

N-MDVA will validate unit IO defensive readiness, as well as demonstrate current and innovative IO concepts and capabilities, in order to meet or emulate evolving threats. Additionally, N-MDVA provides an excellent opportunity for Reserve integration.

Common rules of engagement during N-MDVAs include:

-No planned adverse customer impact from active or passive assessment measures.

-Adversary IO capabilities, tactics and techniques will be portrayed based upon current intelligence driven adversary intent and capability threat assessments.

-Identified vulnerabilities will have corresponding actionable remediation recommendations.

-N-MDVA team will conduct regular after action meetings to identify issues and facilitate timely corrective actions.

-Findings belong to requesting customer organization. Sanitized, non-attributable lessons learned will be forwarded appropriately.

N-MDVA concept of operations continues to evolve through integrating multiple Navy Information Operations Commands' and Fleet Information Operations Commands' capabilities / competencies as well as other collaborative partnerships. For more information regarding N-MDVAs, send an email to OPSEC@navy.mil with subject N-MDVA.

*Article submitted by Daryl Haegley, USN Retired. His last active duty assignment was the Navy OPSEC Support Team OIC and NETWARCOM's Force OPSEC Program Manager located at Navy Information Operations Command-Norfolk. Winner of National OPSEC Individual Achievement Award and DOD CIO Award, he is an Operations Security Certified Professional (OCP) and Certified* Confidentiality Officer (CCO).

*Also view the wikihow article on How to Conduct an Operations Security Assessment: http://www.wikihow.com/Conduct-an-Operations-Security-%28Opsec%29-Assessment*