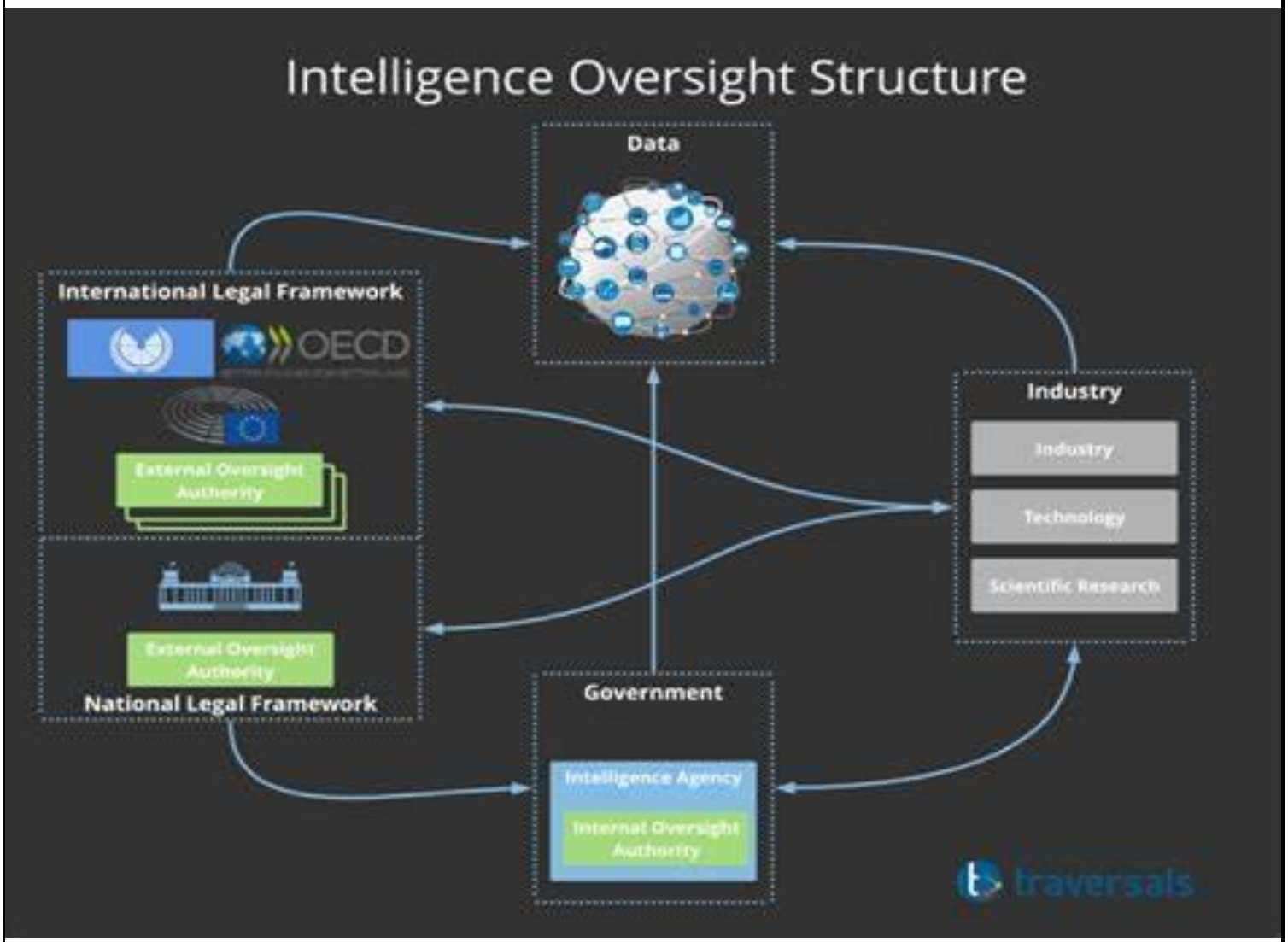
OVERWATCH

"The advancement and diffusion of knowledge is the only guardian of true liberty."
-James Madison

THE JOURNAL OF THE MARINE CORPS INTELLIGENCE OVERSIGHT DIVISION

Volume 11 Issue 1 Fall 2022



A depiction of an Intelligence Oversight Structure

IN THIS ISSUE, FEATURED ARTICLE: EXPANDING INTELLIGENCE OVERSIGHT WON'T BE SIMPLE

Inspector General of the Marine Corps

The Inspector General of the Marine Corps (IGMC) will promote Marine Corps combat readiness, institutional integrity, effectiveness, discipline, and credibility through impartial and independent inspections, assessments, inquiries, investigations, teaching, and training.

The Intelligence Oversight Division

To ensure the effective implementation of Marine Corps-wide oversight of Intelligence, Counterintelligence, Sensitive activities (to include USMC support to law enforcement agencies, special operations, and security matters), and Special Access Programs. To establish policy and ensure their legality, propriety and regulatory compliance with appropriate Department of Defense/ Department of the Navy guidance.

Contact Information

Mail:

Director, Intelligence Oversight
Inspector General of the Marine Corps
Headquarters U.S. Marine Corps
701 South Courthouse Road
Building 12, Suite 1J165
Arlington, VA 22204

Intelligence Oversight Division Staff

GS15 Edwin T. Vogt, Director
LtCol Kira Parrish, Deputy Director
LtCol Bessie Bernstein -Sensitive Activities Officer

Inside This Issue

Web Links

Senior Intelligence Oversight Official (SIOO)
https://dodsioo.defense.gov/

Marine Corps Inspector General
https://www.hqmc.marines.mil/igmc//

Naval Inspector General
https://www.secnav.navy.mil/ig

A Message from the Director

Greetings from the Office of the Inspector General for the Marine Corps, Oversight Division. This edition of *Overwatch* is the second of calendar year 2022. As always, the articles provided in this issue do not represent the opinion of Intelligence Oversight Division or the Office of the Inspector General.

If not aware, we have a new Inspector General on deck. **MajGen Jason Q. Bohm** has been on deck approximately two months and is deeply engaged in the Inspector General process and particularly the Intelligence Oversight portfolio. His vision in a nutshell is to **shift our inspection process from foundational to institutional to meet the challenges of Force Design 2030.** Stay tuned for more updates on this issue.

As many of you have already undergone an inspection with the updated Intelligence **AND** Intelligence Oversight Checklist, you are aware that we are still fine tuning this more rigorous checklist. I want to thank everyone who provided feedback on the efficacy of this update. We have heard your comments and will implement many to add additional rigor. Continue to do your best to uphold the laws and directives that guide our discipline.

Our first article was authored by Ronald Marks who served as Senate liaison for five CIA Directors and intelligence counsel to two Senate Majority Leaders. He is currently a visiting professor at the Schar School of Policy and Government at George Mason University.

The second article by Aidan Poling are the results of a panel discussion. The event focused on how House Permanent Select Committee on Intelligence can adjust its work—and that of the US intelligence community at large—to refocus from counterterrorism to great-power competition.

Next, I am excited to add a new segment for the newsletter entitled Intelligence in History. This will be a collection of historical stories and the use of intelligence disciplines throughout history

The last article by Larry Hanauer is Vice President for Policy at the Intelligence and National Security Alliance (INSA), an association promoting public-private collaboration on intelligence and national security

Semper Fidelis,

Edwin T. Vogt
Director, Intelligence Oversight Division
Office of the Inspector General of the Marine Corps
Ph: 703-604-4518 DSN: 664-4518
Email: Edwin.Vogt@usmc.mil

Featured Article

Expanding Intelligence Oversight won't be simple
Ronald Marks, opinion contributor

According to news reports, Senate Majority Leader Charles Schumer (D-N.Y.) has announced his intention to provide all Senators with staff are cleared to oversee America's intelligence program. As a former CIA Senate liaison and intelligence counsel to two majority leaders, I think he is absolutely right in doing so - but it is a multi-dimensional Gordian knot: more complicated than you might think.

To be blunt, neither of the intelligence oversight committees - the House or the Senate - is really doing the kind of intrusive work that must be done to safeguard the people's money and our national security interests. If anything, in my opinion, there is an increasingly erratic relationship between the committees and the overseen - either too cozy or too hostile.

The intelligence community (IC) is now nearly $86 billion - over three times the size of the late 1990s. This is the size of a Fortune 100 company with a publicly stated employment of over 200,000 people. It is one of the largest parts of the discretionary budget of the U.S. Yet, the numbers below the "top line" are classified, and members vote "blind," trusting the committees do their job with multi-billion-dollar programs that certainly affect Defense Department activities, State Department diplomacy, and Homeland Security.

The IC has also become increasingly involved in high stakes political issues, ranging from sending a CIA director to negotiate with the Russians, to legally asserting itself in extensive intelligence gathering in the United States, to engaging in legally sanctioned attacks against our enemies overseas.

Not a cure-all

The Senators, outside the committees, are about to find themselves in several situations that they may not be anticipating. While it will be interesting and - in my opinion - vital to give a fresh perspective, looking under the hood of intelligence, it will not be without difficulties.

The first is simply clearing staff to the security clearance level required. After 40 years, I can tell you it is an intrusive process. But, you are handling information that can damage your country's security. Thus, the price of glory.

The question will be: How many staff will want to submit to that process? And how many, as we have seen time and time again, may have trouble getting cleared through that process. Drug use, gambling problems, and debt - these are common issues that stop people from getting their clearances.

Another issue is going to be one of access within the Senator's staff. If one person alone is cleared, are they going to report to the Senator alone - without telling the rest of the Senator's senior staff? Ever meet a legislative director or an administrative assistant that wants to be blindsided by an issue?

And, by the way, the information you receive is classified, and your Senator can't talk about it on the floor or otherwise publicly. So, what are you going to say to the reporters and your constituents about what you have learned when they inevitably ask?

There will be the inevitable leaks of information by staff and Senators. That simply can't be helped. But, I must say - in my experience - the vast majority of the leaks come from the executive side.

So, yes, I agree with Senate Majority Leader Schumer and his desire to provide his colleagues insight into how the people's money is being spent in the vast American intelligence community. However, make no mistake, it's going to have its challenges.

Congressional oversight of intelligence for great-power competition

By Aidan Poling

On October 4, the Scowcroft Center's *Forward* Defense practice hosted a hybrid public event on the topic of "Intelligence Community and Intelligence Community Reform." The event was

part of a series sponsored by the minority members of the House Permanent Select Committee on Intelligence (HPSCI) titled *Beyond the SCIF*.

The event focused on how HPSCI can adjust its work—and that of the US intelligence community at large—to refocus from counterterrorism to great-power competition. The experts agreed that the great-power challenge will require a bipartisan approach to intelligence oversight that encourages the adoption of open-source intelligence and places an emphasis on integrating the expertise of other committees.

The event was moderated by Ranking Member Michael Turner (R-OH). The expert panel included Undersecretary Kari A. Bingen, Senior Fellow and Director, Aerospace Security Project, Center for Strategic and International Studies and Former Deputy Under Secretary of Defense for Intelligence and Security; Representative Jane Harman, Distinguished Fellow and President Emerita, Wilson Center and Former Ranking Member, US House Permanent Select Committee on Intelligence; Dr. Matthew Kroenig, Director of Studies and Acting Director, Scowcroft Center for Strategy and Security, Atlantic Council; and Representative Glenn Nye, President & CEO, Center for the Study of the Presidency & Congress and Former Member, US House Armed Services Committee.

Reorienting to great-power competition

The most prominent theme of the panel was the challenge involved in shifting the intelligence community from a mission focused on counterterrorism to collection and analysis for great-power competition. Bingen noted that twenty years focusing on counterterrorism had "atrophied" the intelligence community's capabilities when it came to operating in more contested environments. Kroenig observed that, during the War on Terror, the intelligence community had become very skilled at exquisite data collection and targeting of individual high-value targets. He argued that great-power competition required a shift in focus from data collection to more strategic analysis.

A whole-of-nation approach

Harnessing the aggregate power of the United States to compete with China and Russia has become an increasingly significant focus for policymakers. The panelists contended that HPSCI's approach to intelligence should reflect this. Bingen remarked that policymakers frequently struggle because they only see half the picture, either intelligence on adversaries (the "red team") or on US capabilities (the "blue team"). Emphasizing that information must be more broadly distributed across committees, Harman and Turner suggested that lawmakers would be better off having access to both "blue" and "red" team information.

Importance of bipartisanship

The panelists heartily agreed that a bipartisan approach on the intelligence committee would be vital for effectively conducting its work. The emerging bipartisan consensus in Washington on prioritizing competition with China might serve as a catalyst for future bipartisanship on HPSCI. Nye and Harman both praised Turner for fostering such a spirit in his time on HPSCI, noting that an advantage of HPSCI historically has been its bipartisan ethos.

Harnessing OSINT and new technology

New technology and the rise of open-source intelligence (OSINT) are dramatically changing how the intelligence community should operate. Nye underlined how the Biden administration's release of intelligence before Russia's February 2022 invasion of Ukraine shows how intelligence can be part of information operations. The war in Ukraine is an example of OSINT being actively harnessed by both warfighters and the public to assist in warfighting and shaping the information environment. Harman noted that publicly available commercial satellite imaging has become a highly beneficial source of intelligence. New technologies like machine learning and automated language translation should be better harnessed, according to Bingen, to allow intelligence analysts to make sense of the mass of data now available to them from these sources.

Introducing a New Segment- Intelligence in History

THE CULPER SPY RING

In October 1778, with the Continental Army encamped outside British-occupied New York City, George Washington and Benjamin Tallmadge masterminded what would become the most successful and enduring espionage network of the war. It was named the Culper Ring, an adaptation of Culpeper, the small Virginia community where George Washington had worked as a surveyor in his youth. Though Washington had a limited budget for espionage, he devoted nearly one-quarter of it to the Ring.

Collecting intelligence on British forces in New York City and Long Island, the Culper spies provided Washington with a wealth of secrets about British plans, unit strengths, and defenses. The discoveries aided Washington's efforts to keep the Continental Army intact and bottle up large numbers of British soldiers in New York.

Members of the Ring were subjected to intense British scrutiny, and though several were arrested during the course of the war, not a single member was ever unmasked. Existence of the spy ring was virtually unknown to the public until the discovery of revealing correspondence in 1929.

Among the Culper Ring's espionage successes were its foiling of a British counterfeiting operation to weaken the young republic by devaluing Continental notes. The British had even stolen reams of the paper used in the printing process, adding to the perceived authenticity of the counterfeit dollars.

Ring members also alerted Washington about British plans in the summer of 1780 to ambush 6,000 French soldiers arriving in Rhode Island to aid the Americans. The British had been tipped off about the French landing by their own spy, Benedict Arnold. After informing French allies of the impending attack, Washington ordered his operatives to spread disinformation that he was preparing to raid New York. The British took the bait, choosing to defend the city rather than attack the arriving French forces.

This would not be the last time Washington used deception to hobble his adversaries; he later convinced the British of an impending attack on New York City, thus preventing British forces there from reinforcing the garrison in Yorktown, Virginia.

In perhaps it's crowning achievement, the Ring obtained a copy of the British naval codes in 1781, providing the French Navy with a profound advantage against the British fleet during the Battle of the Chesapeake that year. The French sea victory was instrumental to Washington's siege of the British Army at Yorktown, hastening an end to the war.

Code Names, Ciphers, and Secret Inks

To preclude the British from decoding intercepted messages from the Ring, a number code dictionary was employed, substituting numbers for people, places, and things. This shielded the sensitive components of each message, provided the writer did not reveal important context in the unencoded portions.

The Culper Ring also had access to limited amounts of invisible ink developed by James Jay, a chemist and brother of John Jay. The ink – a unique creation that required a separate chemical reagent to reveal concealed text – was used in letters between the two brothers, and quantities were provided to Washington and others for use during the war.

Intelligence agencies must transform acquisition

Larry Hanauer
October 18, 2022 2:39 pm

The Intelligence Community spends about 70% of its budget — roughly $59 billion in fiscal year 2022 — on contracts with private companies that provide everything from satellites to janitorial services. But IC acquisition is slow, process-oriented and understaffed, all of which delays the procurement of critical services, hinders the adoption of advanced

technologies, and increases costs for both companies and American taxpayers.

To take advantage of private sector innovation, IC policymakers must change acquisition processes to focus on outcomes rather than inputs, enable more unclassified and remote work, make it easier for contractors to clear staff and access secure workspaces, and enhance the acquisition workforce. Ultimately, as the Defense Department wrote to Congress about its own procurement ecosystem in 2017, the IC must adapt its regimented contracting processes to enable critical thinking, effective risk management and flexible decision-making.

First and foremost, agencies should write requests for proposals based on statements of objectives (SOOs), which emphasize outcomes and results, rather than statements of work (SOWs), which specify required inputs, tasks and levels of effort. As the Intelligence and National Security Alliance (INSA) noted in a 2017 white paper on the IC's acquisition process, SOOs empower contractors to develop innovative, cost-effective and efficient solutions to achieve the government's goals. SOOs also make contractors accountable for generating results, thereby reducing the government's risk.

Second, agencies must provide clearances for industry personnel who perform enterprise functions. With few exceptions, only staff providing direct support to contract execution can have their clearances "held" by the contracting agency; as a result, senior executives, lawyers, billing staff and others whose corporate-level work enables classified projects across agencies cannot receive a security clearance. Such limitations unnecessarily complicate companies' support to government clients.

Agencies should develop a formula for providing clearances to such enterprise staff — perhaps a minimum number of slots for any company undertaking classified work plus a percentage of a company's total cleared billets. The Senate Intelligence Committee's draft FY2023 Intelligence Authorization Act requires the Director of National Intelligence to develop a policy for providing such cleared billets; if passed, this provision would greatly enhance contractors' ability to support critical missions across the IC.

Third, intelligence agencies should allow more tasks to be undertaken at the unclassified level. Like other organizations forced to find new ways of operating during the pandemic, the IC learned that a great deal of work — from open source research and analysis to software development — can be performed at an unclassified level. By reducing the amount of work that must be done in secure facilities, agencies can take advantage of telework, provide contractors with greater hiring flexibility, bring new skills to intelligence missions, and lower personnel and facility overhead costs. As INSA recommended in an August 2019 report on the pandemic's impact on acquisition, all contracts should include clauses on the performance of remote work.

Remote work could even be permitted for classified tasks. Contracts often specify that work must be performed in a government agency's secure facility. But many cleared contractors have their own certified secure facilities, and personnel who live far from an agency can often find a desk and a classified email connection in another secure office nearby. Flexibility on where work is performed (as long as security requirements are met) would undoubtedly help retain experienced personnel in the cleared workforce.

Fourth, IC agencies should fund the construction, certification, and operation of shared Sensitive Compartmented Information Facilities (SCIFs) — essentially classified co-workspaces. For a company to build and certify a SCIF, it must have a contract requiring such a facility. This requirement prevents small businesses and non-traditional government contractors (e.g., start-ups and high-tech companies) from accessing the secure workspaces required to do classified work, write a classified proposal, or develop a classified technology prototype. Without access to a SCIF, such companies can't even review classified contracting announcements, and they can't compete for contracts they don't know exist.

Shared SCIFs would enable such firms to enter the intelligence market more easily and at lower cost, thereby bringing new ideas and technologies into the IC. (They would also facilitate remote classified work,

as discussed earlier.) Congress directed the DNI and the Secretary of Defense to create processes for establishing shared SCIFs in section 1628 of the FY2018 National Defense Authorization Act, yet almost five years later, only a handful exist.

The fifth and most complex step that intelligence agencies can take is to enhance their acquisition workforce. The current cadre of government contracting officers (COs) is about 20% below full staffing and, due to retirements and attrition, relatively inexperienced. These challenges make it harder for contracting staff to understand program manager requirements and translate them into contract specifications that are clear, feasible and outcome focused.

The IC should prioritize recruitment, retention and training of acquisition professionals, using flexible hiring authorities to bring in talent (at elevated pay grades, if necessary). Agencies should also encourage the exchange of acquisition personnel with the private sector, which would foster greater understanding of partners' goals, processes and challenges. The congressionally mandated Advisory Panel on Streamlining and Codifying Acquisition Regulations (known as the Section 809 Panel), which examined Defense Department acquisition inefficiencies, recommended flexible hiring authorities and talent exchanges in its June 2018 and January 2019 reports. Its recommendations apply equally well to the IC, which could use the ODNI's new Public-Private Talent Exchange (PPTE) program to manage such professional development initiatives.

Contracting obstacles make it harder for the IC to draw on industry's immense expertise. Given the need to incorporate private sector innovations into intelligence collection and analysis — not to mention the amount of money the IC spends on contracts — intelligence agencies must take steps to make their acquisition processes more efficient and effective.

.

Intelligence Photographs in the News

Photo by Sgt. Kenny Gomez

Major General Jason Bohm, Brig. Gen. Ahmed Williamson, and Sergeant Major Adan Moreno receive a presentation regarding Machine Learning and Artificial Intelligence from Johns Hopkins University Applied Physics Laboratory (APL) staff members at APL's Laurel, Md., campus on September, 22 2021. Marine leaders are researching modernization efforts to support the Marine Corps' force design initiatives of recruiting and retaining talented Marines

(U.S. Marine Corps photo by Lance Cpl. D'Angelo Yanez

Col. Brendon G. Harper, commanding officer of Marine Corps Intelligence Activity, Marine Corps Base Quantico, gives remarks during a change of command ceremony aboard Marine Corps Base Quantico, Virginia, June 19, 2020.

Intelligence Oversight Division

MISSION: To ensure the effective implementation of Marine Corps-wide Oversight of Intelligence, Counterintelligence, Sensitive activities (to include USMC support to law enforcement agencies, special operations, and security matters), and special Access Programs. To establish policy and ensure their legality, propriety and regulatory compliance with appropriate Department of Defense/ Department of the Navy guidance.

Examples of sensitive activities include:

- Military support to Civil Authorities
- Lethal support/training to non-USMC agencies
- CONUS off-base training
- Covered, clandestine, undercover activities
- Intelligence collection of information on U.S. persons

SECNAVINST 5430.57G states**:**

"...personnel bearing USMC IG credentials marked 'Intelligence Oversight/Unlimited Special Access' are certified for access to information and spaces dealing with intelligence and sensitive activities, compartmented and special access programs, and other restricted access programs in which DON participates. When performing oversight of such programs pursuant to Executive Order, they shall be presumed to have a 'need to know' for access to information and spaces concerning them."

WHAT IS INTELLIGENCE OVERSIGHT?

Intelligence Oversight ensures that intelligence personnel shall not collect, retain, or disseminate information about U.S. persons unless done in accordance with specific guidelines, proper authorization, and within only specific categories (*See References*).

DEFINITIONS

i. **INTELLIGENCE OVERSIGHT (IO):** Ensures that intelligence personnel shall not collect, retain, or disseminate information about U.S. persons unless done in accordance with specific guidelines, proper authorization, and within only specific categories. References: E.O. 12333, DoDM 5240.01, DoD Reg 5240.1-R, SECNAVINST 3820.3F,SECNAVINST 5000.34G, MCO 3800.2B

ii. **INTELLIGENCE RELATED ACTIVITY**. Activities that are not conducted under the authority of Executive Order 12333 that involve the collection, retention, or analysis of information, and the activities' primary purpose is to: a. train intelligence personnel; or b. conduct research, development, or testing and evaluation for the purpose of developing intelligence-specific capabilities. Reference: SECNAVINST 5000.34G.

iii. **SENSITIVE ACTIVITIES:** Operations, actions, activities, or programs that are generally handled through special access, compartmented, or other sensitive control mechanisms because of the nature of the target, the area of the operation, or other designated aspects. Sensitive activities also include operations, actions, activities, or programs conducted or supported by any DoD component, including the DON, that, if compromised, could have enduring adverse effects on U.S. foreign policy, DoD or DON activities, or military operations; or, cause significant embarrassment to the United States, its allies, the DoD or DON. Reference: SECNAVINST 5000.34G.

iv. **SPECIAL ACCESS PROGRAM (SAP):** A program activity that has enhanced security measures and imposes safeguarding and access requirements that exceed those normally required for information at the same level. Information to be protected within the SAP is identified by a security classification guide. DoD SAPs are divided into three categories: Acquisition SAP; Intelligence SAP; or Operations and Support SAP. Reference: SECNAVINST 5000.34G.

v. **QUESTIONABLE INTELLIGENCE ACTIVITY:** Any intelligence or intelligence-related activity, when there is reason to believe such activity may be unlawful or contrary to any Executive Order, Presidential Directive, Intelligence Community Directive, or applicable DoD policy governing that activity. Reference: SECNAVINST 5000.34G.