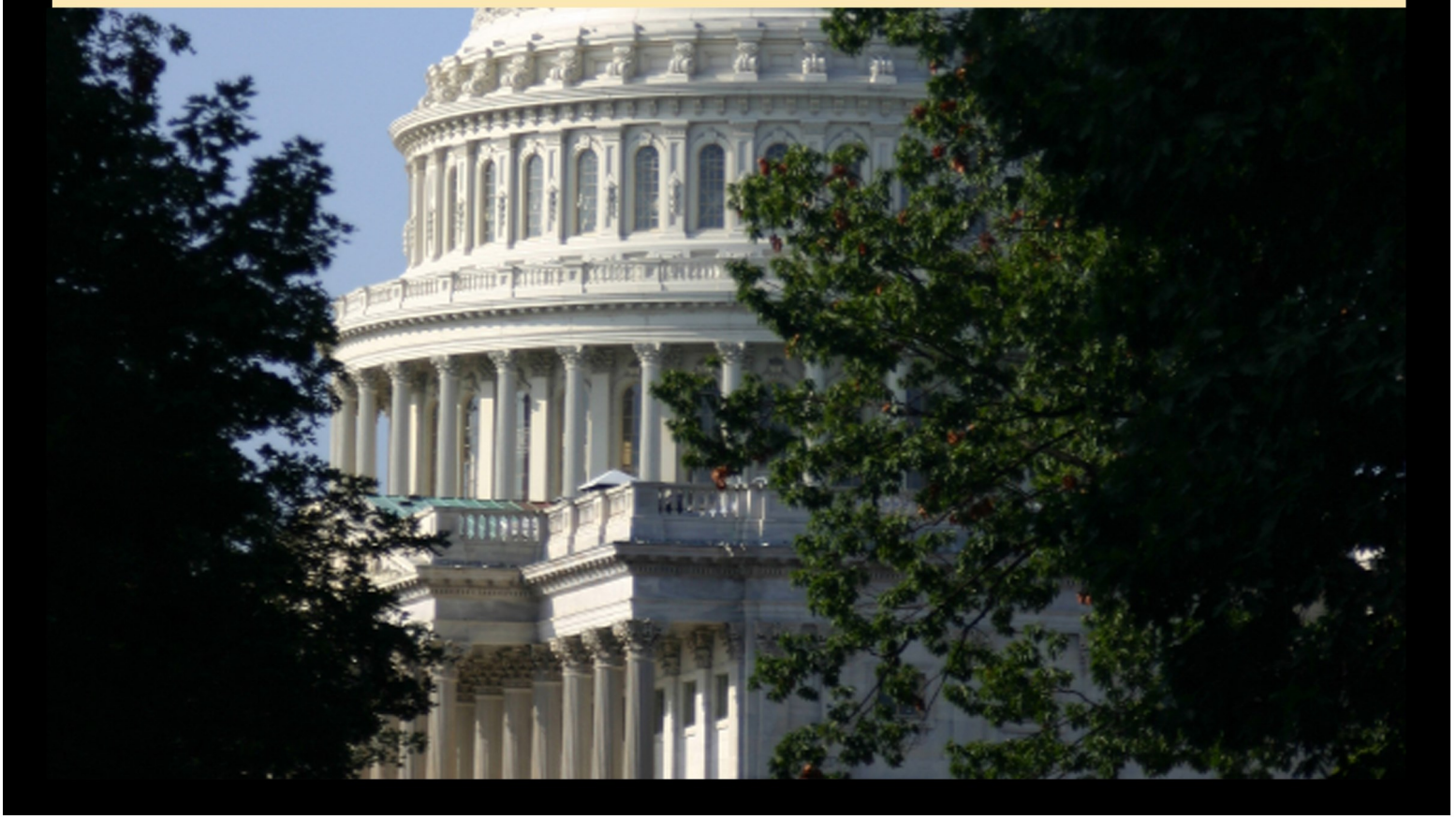
SAM in the Federal Government

"Same... but Different!"

By: **Steven R. Ligon, Ph.D. CSAM**
Senior Systems Engineer, SAM Project Lead,
Intelligence Consulting Enterprise Solutions, Inc. (*ICES)*

By: **Gary P. Feltz, DAWIA PM Lvl 3**
Senior Systems Engineer, SAM Project Deputy Lead,
Intelligence Consulting Enterprise Solutions, Inc. (*ICES)*

By: **Michael J. Schenaker, CSAM**
Senior Systems Engineer, **Intelligence Consulting Enterprise Solutions, Inc. (*ICES)***



Not a Monolith

To listen to the pundits in the media today, one would think that the Federal Government is a monolithic entity, made up of intertwined parts with in-depth knowledge of each other's actions. In reality, while it is large and complex, comprised of intertwined agencies and offices with specific missions, they are not necessarily aware of each other's low-level activities or plans. These authors, with over 100 years of Government and Federal contractor experience, can assure you that Federal agencies are competing for a piece of declining budgets. Such is the case for IT. Each agency and office has for decades been responsible for their own IT and sharing is traditionally anathema to the operations of each.

The intelligence community we serve is comprised of agencies and organizations of the executive branch of the Federal Government. The "big 5" of the US Intelligence Community: Defense Intelligence Agency (DIA); National Security Agency (NSA); National Geospatial-intelligence Agency (NGA); National Reconnaissance Office (NRO) all part of the Department of Defense (DoD); and the Central Intelligence Agency (CIA), an Independent Federal Agency, represent the best known parts, yet are controlled by differing programs in the Federal Budget. The remaining 12 partners come from a wide range of departments such as Justice, State, Energy, Drug Enforcement, Homeland Security, Treasury, and the military services. [1]

The title of this article insinuates that we plan on addressing software asset management across the Federal Government, but that would take volumes. The intent of this article is to present the view from the NGA office that is responsible for Software Asset Management and to which we provide engineering support.

This office was stood up for the first time in May 2011, with the objective of bringing the agency's software resources under management and control. These objectives are being accomplished by centralizing the acquisition of software from numerous integrators and programs to a single office, pioneering the use of a commercial off-the-shelf (COTS) automated Software Asset Management tool, and fielding tools to provide rigorous documentation and discovery of the current software asset inventory. Additionally, we have instituted, policies, processes and procedures based on the principles of SAM found in ISO/IEC 19770 and IAITAM SAM Best Practices.

The views expressed herein are those of the authors, and do not necessarily represent the views of the US Government, or the views of those we serve.

SAM Challenges

IAITAM divides the scope of SAM into eight categories: Acquisition, Vendor, Financial, Documentation, Legislation, Asset Identification, Compliance, and Disposal Management. [2] To keep this article to a readable length, we decided to focus on those with the greatest challenges to the federal sphere: Acquisition Management - Requirements Definition (Pre-Acquisition part of Acquisition) and other general Acquisition Management Challenges; Legislative Management focusing on unique regulatory and policy challenges to federal contracting and agency support; Vendor, Asset Identification, and Compliance Management challenges.

Acquisition - Requirements Definition

Agencies have multiple missions and responsibilities. NGA is responsible for making the maps, charts, models, and imagery analysis to fight wars, track terrorists, guide emergency responders to where they are needed, support other intelligence agencies in tracking technological, cultural, physical, geographic, gravimetric and geodetic change, as well as provide cutting edge capabilities for geographic information systems. All of these mission spaces use software, but the amount of common software support is less than half of the inventory that the Agency uses. The remaining missions are supported by conglomerates of niche and specialty software. This software is often quite expensive to maintain, cost prohibitive to replace, and requires maintenance of older and outdated operating systems.

This complicates alternatives analysis, as seldom does one vendor's software replicate all of the mission-related functions of a system of systems that has been custom integrated. However, in an era of ever-declining budgets and ever-increasing mandated spending cuts, the agency finds it must move to lower and no cost options as much as possible to have the fiduciary resources to support the maintenance of mission-specific application conglomerates required fulfilling those missions.

NGA is doing this largely through analysis of alternatives on large-cost requests for software. NGA's SAM office is now squarely in the review and approval cycle for all

large cost change requests, and requests for new software to support new acquisitions. As we provide a true lifecycle cost of the requested software, we can now suggest alternatives, identify unused inventory and suggest low and no cost alternatives which, when enacted, allow the agency to avoid unneeded software expenditures.

General Acquisition Challenges

The Federal Government has tried to address acquisition reform for decades with the goal of cost savings, reductions in duplication of agency activities, and addressing Total Cost of Ownership (TCO). So far, acquisition reform has done nothing to shorten the timelines or the acquisition steps to make the software purchase processes more efficient. The Office of Management and Budget (OMB) and the Federal Acquisition Regulation (FAR) govern agency IT investment decisions. At NGA, the typical software acquisition procurement package consists of a business case with exact requirements, contractual terms and conditions, an Independent Government Cost Estimate (IGCE), a Justifications and Approvals (J&A) statement, potentially a Determinations and Findings (D&F) document and funding by correct appropriation type. This package is reviewed and approved by legal counsel, financial managers, and contracting officers. It can take an inordinate amount of time to complete the package for large vendor contracts, staff for funding, legal, contractual review, and negotiate a final agreement.

Funding enterprise software agreements can be an issue in the federal government as compared with commercial companies. Commercial companies rarely use contractual methods that require up-front funding whereas the agencies' contracts usually require up-front funding. [3] Commercial organizations have an advantage in maintaining competition by identifying, through rigorous technical evaluations, two or three vendors with products that meet their needs. Conversely, the federal government selects one vendor's set of products and competes amongst a set of software resellers for which pricing is negotiated with the vendor. This often means commercial companies get deeper discounts than the federal government.

Legislation Management

One of the big issues with Federal Government contracting is budget uncertainty in funding IT services that includes sustainment of existing software license agreements. Congress has passed sequestration, continuing resolutions, and other funding bills that impact agency funding levels year to year. Under continuing resolutions, the funds trickle into agencies potentially limiting the use of funds prior to receipt of funding authorization. This can lead to late payments to vendors, reinstatement fees for the government, and force de-funding of maintenance to support other mission priorities that may prohibit payment of maintenance at all.

Some government policies are helpful in controlling IT costs. In 2004, the OMB issued a policy for federal agencies to maximize the use of Government Services Agency (GSA) and the Department of Defense (DoD) enterprise software programs through the GSA SmartBUY and DoD-ESI vendor agreements. Both of these initiatives sponsor pre-negotiated software vendor blanket purchase agreements (BPAs) and Enterprise License Agreements (ELAs). These programs offer lower administrative costs in placing orders, minimal documentation requirements, satisfy all FAR requirements for open competition, and permit the use of government credit cards. However, in practice, the paperwork leading up to the procurement is often as cumbersome with or without these efficiencies, and they really don't save much time and effort in the acquisition.

Vendor Management

Conflict between vendors and agencies is no different than between vendors and commercial clients: the vendor's objective is to sell as much as they can, and the client's objective is to pay as little for IT as possible. However, sometimes within the intelligence community (IC) there are unique difficulties encountered when dealing with vendors. For example, vendors are not briefed on the agency's internal policies, processes or procedures for SAM. This poses a major impediment to building a mutual trust between the vendor and the customer. While centralization of software acquisition appears simple enough, vendors continue to approach elements of the agency trying to sell more. This levies an internal requirement to educate the various members of the federal agency in SAM responsibilities and how they impact the IT directorate as well as their respective offices. This impact also extends to the Chief Information Office (CIO), Office of General Counsel, Office of Contract Services, and Financial Management

Services. And finally, the move towards an intelligence community-wide IT Environment (IC ITE) [4] brings with it a host of vendor and reseller representatives already working with a single IC partner, not knowing all the other customer requirements or their mission spaces. This is compounded as the IC continues to collapse similar software contracts into one contract vehicle. In the end, the onus of building the mutual trust must come from the collective SAM representatives working together within the intelligence community.

Asset Identification

Due to the unique nature of our supported customer's IT environment, there are many challenges to asset identification, especially for discovery and inventory management. Some are common to the commercial sector, such as multiple operating system (OS) environments, remote sites, disconnected operations, Continuity of Operations capabilities (cold or warm), immature adoption of ISO 19770 standards for naming conventions and software metadata tags, absence of a single tool that can discover all software deployed and levels of use, and mobile devices. Others seem to be unique to the IC, such as multiple domains based upon information classification levels and isolated enclaves. Hundreds of mission-specific integrated systems comprised of numerous applications, managed by various Program Management Offices and sometimes multiple service providers deploying software across all or portions of this IT environment add to the confusion. And finally, the transition to a common IC Desktop Environment (IC DTE) [5] leveraging both shared ELAs and IT infrastructure between 17 IC components is presenting its own and sometimes unique set of challenges (e.g., adopting common applications, disparate machine naming conventions, lack of standards in network construction, conflicting firewalls, etc.).

Compliance Management

Unlike the overwhelming oppression of ceaseless audits many of our industry counterparts experience, in the IC we are not exposed to such an onslaught. Instead, we are being asked more and more for what we have and what we are using. We have quarterly mandatory reporting to Congress and DoD on software, and will be subjected to a DoD-wide IT asset audit in FY16. Much of our software inventory lies behind security firewalls and is laden with classification control and access management that gives NGA control over what data is exposed to a vendor given current legal mandates. However, this "great wall" brings with it an increased responsibility as stewards of the public trust to control our own world and to develop a legacy of documentation that assures the vendor that we are trustworthy stewards.

While it is rare within our supported customer's environment to find non-compliance due to software rental, hard disk loading, counterfeiting or internet piracy, the risks lay more in the challenge of running parallel environments at different classification levels and understanding the various terms and conditions of the licenses. Some software license contracts grant multiple domain access to each user and as such, one license may be assigned to multiple domains for a single user based on the assumption the user is only using one domain at a time. However, other licenses define use as one license for each user on each domain. While not impossible, it does present a challenge with roughly 17,000 users spread around the globe on numerous internal and external domains. Rigorous attention must be paid to each application (of which we use over 3,000) to ensure that compliance. We are constantly researching and implementing tools (at additional cost) into our environment that aid in pairing the license inventory with the assets identified. But, set up time is slow and requires many staff hours of data entry, contract scrutiny to ensure that proper constraints are entered correctly in that tool, and data quality verification. Additionally, because of the multiple domain issue, identification of other discovery tools is becoming more important, especially as many of these licenses are being used in the IC DTE and by law, must be segregated from other agency licenses to comply with "Anti-Deficiency" provisions that prohibit one Agency from buying for another.

NGA is instituting the industry best practice of establishing a routine internal audit of its software inventory which will greatly increase the attention to detail required to enforce intellectual property and to give transparency to vendors into our processes and results while maintain the security of our classified networks.

Transforming the IC IT

Like most of the IT asset management community, federal asset managers are wrestling with how to control both their hardware and especially their software inventories in the cloud.

In 2012, under the leadership of the Office of the Director of National Intelligence (ODNI), the IC initiated a strategy to transform their IT environment in order to; build a survivable infrastructure, have standards-based interoperable enterprise architecture, enable a collaborative analytical environment, and provide a set of tools to support standardized business processes. This effort, the Intelligence Community Information Technology Environment (IC ITE) is currently defined in "IC ITE Strategy 2016-2020". [6] Part of this strategy is to leverage proven cloud technologies to achieve aspects of its three goals. [7] To date, there are two cloud instantiations supporting IC ITE. They are:

GovCloud: established in 2013 by the NSA acting as the designated cloud prototype engineer, this cloud provides a scalable, accessible and secure cloud-computing environment available on demand for the entire IC. NSA acts as the cloud service provider to the other IC members. It combines open-source and commodity software designed to provide a "repository of choice."

Commercial Cloud Services (C2S): in an effort to reduce the estimated $ 8 billion spent on IT within the IC, this multi-million dollar public cloud built on private premises is based on Amazon Web Services specifically for the IC and is managed by the Central Intelligence Agency. C2S "…is capable of analyzing 100 terabytes of raw data on a cluster at a time. The CIA cloud will employ a MapReduce-based system to spread big data loads out over multiple clusters for simultaneous processing…. MapReduce came out of a Google approach to mapping data out to a server cluster, then assigning analysis work based on which processor was closest to the relevant data. It's a way to use commodity servers with limited storage attached in a large-scale and high-speed manner. [8]

Other government agencies, "including NASA, the GAO, the U.S. Army, and the Recovery Accountability and Transparency Board, which powers the Recovery.gov stimulus-tracking website, already use Amazon's cloud services [and]…more are expected to follow as they try to meet the requirements of the Federal Data Center Consolidation Initiative…[that] seeks to close 800 federal data centers by 2015. [9]

IC Desktop Environment (IC DTE)

Part of the overarching IC ITE initiative is to deliver a common suite of desktop applications. IC DTE provides access to common services, and is supposed to eliminate "stovepiped" or redundant systems without sacrificing flexibility or survivability. Grant Schneider, DIA's CIO, summarized the objective of the DTE:

> We are talking mostly TS/SCI (Top Secret/Sensitive Compartmented Information), so when we talk about having a common desktop environment it means that you [an authorized IC employee] will be able to go anywhere — certainly within the big five agencies to start [NGA, DIA, CIA, NSA, and NRO]— sit down at any TS [top secret] workstation… log in, authenticate to the system … and … get access to your e-mail, your home directories, your shared files, etc. So we will add mobility across the agencies, whereas today we really are immobile within our agencies, for the most part…It's also going to help facilitate information sharing because we're now going to be moving towards an environment where we will do security and tagging of data at the data level, as opposed to the network level. [10]

This IaaS (Infrastructure as a Service) supports a variety of thick, thin and mobile endpoint devices. It is managed by a Joint Program Management Office (JPMO) currently consisting of DIA, NGA and ODNI personnel directed by Ms. Kendrea DeLauter of the Defense Intelligence Agency (DIA). [11] The effort is being conducted in phases, with Phase 1 scheduled to conclude at the end of FY15 and Phase 2 ending in FY18. To date, IC DTE has over 9,000 users on a common desktop environment, offering over 460 applications and widgets to users. It is hoped that this environment will make it easier to create ad hoc virtual specialist teams, decrease IT management costs, enable more frequent tech refreshes, and ease training time and expenses. [12]

Changing Contracting Strategies

As discussed earlier in this article, there are federal laws and policies that govern contractual agreements of IC agencies. IC software agreements are very similar to

those used throughout commercial industry; ELAs, BPAs, End User License Agreements (EULA), etc. However, the advent of the IC ITE has brought about a new way to leverage these agreements. Generally referred to as "IC-wide license agreements," these agreements are ones in which a specific agency "owns" the contract and the other IC members acquire software off of that contract. Some vendors have agreed to allow permanent reassignment of their licenses and attendant maintenance to other IC partners, but this is at the discretion of the vendor. Standing up the initial IC-wide contract (DIA/NGA with Microsoft) was a heroic effort by both vendor and customer. It set a process in place that is now being replicated throughout the IC as the Office of the Director of National Intelligence (ODNI) assigns vendors to the IC partners to negotiate the IC-wide contracts. For the taxpayer, this means that only one agency is doing the negotiating instead of 5 with the vendor, reducing the level of resources required and related costs.

However, IC-wide agreements bring with them certain challenges, such as relying on another agency staff's negotiating skills and experience to get the best value, making sure that the terms and conditions will be satisfactory for all agencies, and all agencies will identify comprehensive future needs in order to set caps and ceilings in the contracts.

Meeting the Challenges

As illustrated in this article, much of the complexity we face in the federal sector is analogous to the commercial sector. The nuances are subtle, and reflect complications imposed by being stewards of the public funds. The impacts from declining budgets and Continuing Resolutions can complicate software acquisition management, especially during the first quarter of each fiscal year. The parallel domains that segregate security enclaves make enterprise asset identification, audit, and compliance verification very complex. On the other side, those same security environments provide some control over the timing of vendor audits and reduce the turbulence experienced by our commercial compatriot's environments.

Since the inception of SAM in NGA, millions of dollars of cost avoidance have been realized due to centralized software acquisition. The agency, formerly

characterized by numerous, uncoordinated software acquisitions, has a more stable IT environment with greater understanding of what it acquires in light of what it already owns. Intellectual property is better managed today because NGA works to better understand license contract terms and conditions. It also can better analyze their implications as we move to the cloud. Overall, the agency is far better off today because it has implemented SAM. New challenges such as moving to cloud environments will bring not yet fully understood changes to software license, legal, financial oversight and compliance management. But, because the agency has implemented SAM, NGA is better prepared to meet those challenges.

Notes

[1] ODNI, Members of the IC (access on 27 Jan 2015): http://www.dni.gov/index.php/intelligence-community/members-of-the-ic

[2] Chapter 5: The Scope of Software Asset Management, in CSAM Certified Software Asset Manager Manual, IAITAM Publishing, LLC, 2008, 29-32.

[3] Strategic Business Process Reengineering Initiative (DASW01-96-0067, TASK 5), Best Practices for Enterprise Software Agreements Within DoD and the Corporate World, September 14, 1999, DoD, 2, 11, 17-18.

[4] Detailed below in "transforming the Intelligence Community IT Environment – see IC ITE.

[5] Detailed below in "transforming the Intelligence Community IT Environment – see IC-DTE.

[6] ODNI, IC ITE Strategy 2016-2020, On Line: http://www.dni.gov/files/documents/CIO/IC%20ITE%20Strategy%202016-2020.pdf).

[7] The three goals of IC ITE are: 1) Enhance intelligence integration; 2) Optimize information assurance to secure and safeguard the IC enterprise; and 3) Operate as an efficient, effective IC enterprise. Ibid.

[8] ibid.

[9] Charles Babcock, "Amazon Wins Best Cloud in Bake-Off", Information Week, 6/25/2013, on line: http://www.informationweek.com/cloud/infrastructure-as-a-service/amazon-wins-best-cloud-in-cia-bake-off/d/d-id/1110504?itc=edit_in_body_cross

[10] Barry Rosenburg, "DIA Takes the Lead on Developing a Common Desktop Environment", Defense Systems, May 13, 2012, on line: http://defensesystems.com/Articles/2012/02/28/Chief-View-Grant-Schneider-DIA.aspx?Page=1

[11] http://archive.federaltimes.com/article/20140703/FEDIT03/307030011/IC-moves-toward-common-desktops

[12] http://fcw.com/Articles/2014/09/18/DNI-CIO-joint-IT.aspx