Federal Identity Credential and Access Management (FICAM) and Cloud Email Initiatives

THE RELATIONSHIP BETWEEN EMAIL AND FICAM

What else is 'Email' and how does that definition intersect with Cloud Email? How does all of that intersect with FICAM? Put quite simply, Email is likely to be the most ubiquitous representation of Organizational Identity within an Agency, with additional security relevant data that is important to Organization Security Architectures and services.

Email is typically comprised of an account for each network-enabled user, with some users having multiple accounts to address Agency needs imposed by their Organizational Role (e.g., the user account and the IT Admin account). In modern day IT service models, email is also a collaboration tool used within business processes for establishing meetings, managing address books, creating and managing distribution lists, and similar business functions that we simply take for granted today. Email systems incorporate Organizational relationships (e.g., a mapping of employee to supervisor). They provide notification services based on Distribution Lists that require specific *Identities* to be kept aware of mission critical issues as a function of their job duties. In short, Email Systems are an unintentional Agency Identity Management System.

Linked to this is an architectural intersection present within any Identity Management System – a Security Management capability. This adds further complexity to Email Systems, in that, the directories and repositories that store their *Identity* data are riddled with security data and metadata about Agency users. We can see smatterings of security management in commonly accepted (and typically mismanaged) Security Groups that are used to grant access rights to select users based on their presence within a defined Security Group.

FICAM is Segment Architecture that is wholly invested in the management of identity and security management lifecycles. Therefore, the relationship of an email system and FICAM quickly becomes obvious: ***Email systems are perhaps the largest and most important application for FICAM enabling solutions*** to address, exploit, and support within an Agency. There are several reasons and examples that demonstrate this to be factual:

- Your email systems are probably already tightly integrated with your Identity and Access Management (IAM) capabilities. In some instances, there may already be an IAM System in place, and there is most certainly a connection between it and your Email System. In fact, if your employees enjoy single sign-on to their email accounts (i.e., network logon and seamless access to email), that is all the evidence needed to demonstrate tight integrated connectivity between email and IAM.
- Users that enjoy the capability of using integrated calendar functions, access to other applications, and an ability to collaborate with email based collaboration tools demonstrate another example of how your email solution is tied to IAM in some capacity or another.
- Users like to check their email from several locations and over several devices, which is a federated access to service. For example, users will check their email on their work computer, using their smart phones, or even from their home computers. This demonstrates yet another level of integration between email and IAM.

The link between IAM solutions and Email Systems has become so common in practice that the relationship (for some) is not obvious. However, when contemplating a move of email capability from internal to the Agency to an external Service Provider, this link becomes more obvious by

©2013 LS3, Incorporated.

the second, and in many cases can become an ominous situation to deal with to ensure successful service migration. The ominous aspects are those that are directly related to identity and security lifecycle management. Since the integrated relationship of Email to IAM within Agencies are so commonplace, Agencies typically do not consider the ramifications or impact to organizational security due to underlying dependencies within the Email Systems, nor is it immediately obvious the impact to overall business operations since the Agency has served as its own *Identity Provider or IDP* without giving that notion a second thought for a very long time.

IDENTITY PROVIDERS AND SERVICE PROVIDERS

Identity is the core of any business service offering. In order to know what service you can provide to an *Entity*, you must first know its *Identity*. For example, should you want to extend a business service to an *Entity*, such as providing access to a Reporting Portal to extract business data, you must first understand **'Who'** is requesting access. From there, a determination can be made as to whether they have appropriate security rights/entitlements to access this service, and **'What'** level access they should be provided. Without a proper representation of *Identity*, no business service can be realistically controlled, monitored, or provided. In this example, a legitimate user, whose identity can be clearly ascertained, can be matched up to Access Control information to permit or deny their access to a Reporting Portal service.

In addition to identifying the *Entity* that desires (or needs) business services, there is the fundamental concern for authenticating this *Entity*. That is to say that the *Entity* must identify itself with an appropriate security mechanism (e.g., password, PIN, etc.) to demonstrate they are who they claim to be. This allows appropriate trust in *Identity* to permit/allow desired access. The selected mechanisms can offer varying levels of assurance in (or for) the identity, which is necessary to addressed defined risk associated with granting access to business services or data. For example, where a person seeks access to public data on a web site, there may not be stringent security mechanisms in place to control access. Similarly, where a person is seeking access to highly confidential or even National Security data, a much stronger mechanism may be required, such as a Personal Identity Verification (PIV) Card or DOD Common Access Card (CAC).

Agencies have long served as their own *Identity Provider*. With the advent of '*Cloud*', this is beginning to change. Service Providers are more aggressively seeking to offer Identity as a Service for Agencies with either direct offerings to do so or with subtle identity management capabilities such as those embedded within a Cloud Email (or Email as a Service [EaaS]) solution. However, there are a number of considerations Agencies should review prior to adopting *IDP* as a service. This is true regardless of whether it is directly offered or indirectly integrated into Cloud services.

Service Providers, inclusive of EaaS, seek to provide lower cost solutions for the targeted business services being offered. A *Service Provider* is an external party that seeks to provide a capability to an Agency, typically a vendor that offers a service for a fee. Obviously, to make good business sense, the fee for service model must promise a lower overall Total Cost of Ownership (TCO) with the core services being offered. However, the manner with which a TCO calculation is performed is an additional key consideration that Agencies must consider, prior to making the leap with an expectation for high Return on Investment (ROI).

CLOUD EMAIL AND FICAM/IAM CONSIDERATIONS

Where Agencies seek to engage in Cloud Email/EaaS, there are a number of things that should be fully considered as part of the migration or adoption planning. These items may not be

©2013 LS3, Incorporated.

obvious, but can serve as cost drivers for TCO and ROI models, and therefore warrant a degree of due diligence. The following items should be fully considered:

1) **The FICAM Dependency and Cart Before the Horse –** The most important consideration for Agencies is the dependency associated with adopting "Services in the Cloud" with identity and security lifecycle management (i.e., FICAM). Agencies that engage the Cloud will rapidly encounter architectural intersections and service dependencies on IAM/FICAM. In fact, Agencies may find Cloud Email will serve as the single largest FICAM challenge! This is based on ubiquity of Email services and user and business service dependence on core email services and extended business productivity capabilities that are required today to allow employees to accomplish their day-to-day responsibilities. Inadequate focus on FICAM prior to engaging in Cloud Email will likely result in establishment of point-up or one-off solutions to address unintentionally myopic understandings of Enterprise Security need (e.g., Federation services that only address authentication services). Later, the Agency will discover the remaining needs which will most assuredly result in a constant refactoring and re-evaluation of Agency requirements, costly analysis and reviews of in-place solution(s), and ultimately the establishment of "correct" solutions related to holistic FICAM capabilities that will NOT be able to leverage the point-up or one-off solution that was put in place. It only yields a situation where Agencies find themselves in expensive "rip and replace" approaches to addressing the more accurate set of requirements to support business services, ultimately wasting time, money, and effort on short sighted solutions that are part of an "easier path to accomplish project level need" but that omit broader Enterprise concerns. Capability to engage in Federated Identity Management, Federated Authentication, and other types of related services falls at the "top of the IAM service pyramid". That is to say that these capabilities are built up from architectural Service Models that serve as foundational elements within a well-planned architecture. Agencies should resist the temptation to pour investments into Federation services (e.g., SAML Assertions, WS-Federation, Credential Exchange frameworks) until they have a firm grasp on the underlying Service elements required to allow them to maximize the return on that investment and fully understand how they are controlling and managing the identity and the security lifecycles for the Entities/Identities they manage and serve.
2) **FICAM Strategic Alignment within an Agency** – Since FICAM is a Segment Architecture; it requires appropriate Executive sponsorship, long term investment, and varying levels of subject matter expertise to realize success. Agencies should seriously consider their alignment of FICAM with the IT Strategic Plan. Ownership and responsibility must engage the correct manager (or management group), as assigning responsibility to the incorrect personnel will seriously curtail achievable value. As part of the Federal mandate, an Agency Lead Official should be assigned. This should be an individual with appropriate Agency influence and capability to clear technical, business, and political hurdles/challenges expected within FICAM implementation efforts.
3) **Identity Provider Versus Service Provider** – Agencies should immediately recognize that the relationship between the *Identity Provider* and the *Service Provider* have been long taken for granted as a product of modern day computing. COTS product vendors have fully integrated specific architectural functions as a means of providing user convenience, best-in-class service models, and end-to-end business productivity and operations. They have done this to remain competitive with products they bring to market. In no way should it be deemed a 'hidden ploy' or some major conspiracy to bind organizations to their capabilities or

©2013 LS3, Incorporated.

services. The practice has been common place for a very long time, and it's merely a product of bringing the best products and capabilities to market with sufficient value-add to organizations to attract them to buying their business productivity products. Still, with the outsourcing model of *Cloud*, it widens the obvious nature of this integrated capability and starts to polarize the difference between the different types of *Providers*. Therefore, the Agency must engage risk management and architecture decision making processes to fully understand their role in a Cloud offering, and the impacts associated with that decision.

4) **Hidden Costs in TCO** – It is incumbent upon the Agency to preserve its own interests for managing costs and budget, and is wholly unfair to expect a commodity *Service Provider* to fully understand all of the business processes or organizational dependencies resident in "As Is" capabilities currently enjoyed by the business user. *Providers* typically engage TCO models that provide a cost analysis based on apples-to-apples comparisons. The TCO models examine the cost to provide core business service, such as email services; however, omit underlying dependency costs that are not obvious such as with Identity and Security Management. These can become hidden cost factors that drive TCO models much higher than what a *Service Provider* is representing. Further, addressing management disparity between internal and external security management can result in substantive investment/budget need, particularly when the needs become reactionary a situation where it is "too late" and external services are already adopted.
5) **No Way Out?** – A common error in program planning (and associated budget planning) is lack of examination for the exit strategy from *Service Provider* or *Management Service Offering* capabilities. Agencies are so concentrated on getting a capability set up and in place, that they omit planning to consider solution portability to alternative *Providers*. Unfortunately, this drives budgets so egregiously that the Agencies results in a Vendor Lock situation, where any attempts to port services to an alternative Provider will result in any attempt to migrate cost prohibitive. The ROI needed to adopt a cost competitive Service capability is so high that Agencies cannot take advantage of them and therefore they inadvertently curtail the ability to maximize benefit in lower cost options over time. Want proof you say? Ok. Have you ever considered migrating your current PKI Shared Service Provider from Provider A to Provider B? How about any existing PIV Credential issuance capabilities? Have you ever examined what it would take to move from an existing Provider to a new Provider and what the impact would be to the organization as a function of engaging in that move? Suffice it to say that adoption of Cloud will most certainly lock many Agencies into perpetual mortgages with No Way Out, if the Agency does not provide planning over longer term lifecycles to address and manage this as a critical planning concern.
6) **Identity, Security, and the Cloud** – The primary consideration for security as it pertains to Cloud Services is retention and control surrounding *Identity*. As stated previously, *Identity* is a core dependency for business services and is the foundational element of organizational Security. Though vendors are seeking to provide *Identity* as a Service, there are certain management considerations that should be examined prior to adopting this capability. Outsourcing *Identity* can introduce issues with other business processes and services, based on service/performance variables such as availability and reliability. Additionally, where an outsourced *IDP* engages business decisions to alter the structure or definition of *Identity Data*, which can occur over time as a function of their internal business planning or needs to engage in cost cutting approaches to service management, the Agency can quickly find itself

©2013 LS3, Incorporated.

in a situation where that change to *Identity* can have a ripple effect across many business processes and services, often times with significant cost, performance, and quality impacts.

7) **How Many 'Credentials' Do You Need? –** Identity services are offered today by *Credential Service Providers (CSPs)*, all of which are getting in on the *Identity* as a Service game. There is definitely a market for these services when considering service models such as Federated Identity Management or Federated Authentication, which are promoted in FICAM Segment Architecture (e.g., recognition of PIV credentials cross-Agency to drive down Federal government operating costs). However, Agencies need to give serious consideration to how many 'credentials' they want to support, since each of these credentialing capabilities has an associated identity management lifecycle. Agencies will require investments to support tracking and managing to these credential lifecycles to ensure that their integrated offerings within their business services can sustain proper operating models and adjust to changes that will occur in the Credential's operating lifecycle[1]. These investments may even be nominal on an individual CSP capability, but operating models where the Agency supports ANY credential across broad credential exchange frameworks can multiply individual nominal investments to models that begin to add up quickly.
8) **Identity Management Best Practices** – As a best practice, Agencies should never relinquish ownership and control over *Organizational Identity*, and instead should engage in *Identity Provisioning* approaches that preserve management of *Organizational Identity* internal to the Agency. This approach permits recovery in a situation where a *Service Provider* imposes changes on *Identity* data models or services that do not align with the Agency roadmap or business services. The best practice for Identity Management requires a full understanding of how IDM is addressed within the Agency first, and only then engaging *Providers* with the full understanding of how those services intersect architecturally with the Agency management model. This permits a no surprises approach to service management and permits the Agency to retain ownership and control over their *Identity* data, resulting in flexibility to align business and security services over time as needs are identified.
9) **The User Experience** – The User Experience of Cloud Email is a major consideration with the adoption of service because the user experience is very likely to change. IAM services available for externally hosted capabilities will most assuredly impact the user Single Sign On experience in one way or another, or will drive significant architectural considerations that the Agency must accept to preserve current user experience. These experiences are in and above the user experience when adopting a different vendor solution with a different operating model (e.g., Google Mail versus Microsoft Outlook/Exchange services).
10) **Synchronization and Federation Needs** – local security models within a *Service Provider* may not readily address or match up with Agency standard security service interfaces. Further, application level privileges will need to be appropriately synchronized via *Federated Provisioning* to offers real-time access control capability for to permit access control decisions by individuals within the organization with the authority to make those decisions (e.g., Application/System Owners). Typically, *Service Providers* do not provide robust granular capability in security management, as these services are not core to the business

[1] Risk Assessments, Risk Management Plans, Risk Acceptance, Security Reviews, Interconnect Security Agreements, and related FISMA and NIST required activities are all items of cost in program budgets and are required as a function of providing security capabilities within an Agency.

©2013 LS3, Incorporated.

offering, and therefore the Agency will discover security management burdens that have to be addressed as a function of adoption of new Cloud service models.

CUSTOMER CASE STUDIES

There are several customer case studies that can be offered to demonstrate lessons learned and best practices. Moreover, these lessons can be leveraged to side step poor practices and engage in forward looking planning that ensure Agencies maximize on value received with planned investments. They further emphasize need to appropriately align strategic planning with FICAM, and to engage infrastructure level investments to mitigate Agency risk, maximize investment returns, and preserve Agency security posture with modern Cloud computing capability.

The Department of Labor made a tremendous investment in Enterprise IAM. In 2010, DOL solicited Industry to engage a Best V Offeror to serve as the Agency *FICAM Solution Integrator*. The contract sought to establish a Department-wide FICAM solution. After two long years, and establishment of all of the FICAM infrastructure capabilities required to address FICAM Use Cases, an Agency Manager made the decision to abandon the investment and engage alternative solutions that focused solely on *Cloud Email*.

The original structure of the DOL IAM Program reported directly to the Office of the Chief Information Officer (OCIO) and had an Executive that served as the Business Sponsor and *Agency Lead Official*[2]. Upon departure of this Executive from the Agency, the FICAM Program was reassigned to DOL's IT Operations Group in October 2012. This Program ownership change substantively altered Program alignment and diminished FICAM importance – so much so that the broader Enterprise vision and scope of FICAM was diluted and diminished down to the lowest common denominator of technical components for providing Federated Authentication in support of *Cloud Email*. Additionally, the new Operations focus drew attention away from critical dependencies for ubiquitous enterprise services which impedes value from FICAM; significantly hampering Agency ability to "*go to the Cloud*" with other services. The Operations focus instead sought to focus on long standing and long unresolved IT network management concerns rather than on FICAM solution needs, thus weakening the capability to engage the Cloud, such as:

- DOL's IT Operations Group has long struggled with Network Management, having to support an Enterprise network that suffers from models of disjointed fragmentation[3]. Service segments across the Enterprise could not support ubiquity in Infrastructure Services required in Cloud initiatives and for FICAM capability. These real world limitations and DOL's inability to address them made it impossible to interconnect FICAM services with any level of ubiquity, performance, reliability, or sustainability.
- DOL's IT Operations Group has long suffered with a network environment that supports dozens of Active Directory and MS Exchange mail service domains. Efforts to appropriately consolidate Domains have not been successful, despite investments that

[2] *Agency Lead Official* role is defined in *OMB M-11-11 – Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors.*

[3] Agency firewalls result in establishment of multiple network enclaves and prohibit a single Agency network that can be managed; communication paths that allow sustainable services for end-to-end service models; etc.

©2013 LS3, Incorporated.

have been ongoing for years. The disparity in mail domains result in a disjointed set of *Identity* data that is difficult to resolve as an underlying FICAM need or dependency. This requires individual "*connectors*" to each Identity domain to resolve. Combined with the DOL's inability to resolve simple network challenges, IT Operations was unable to secure proper communications paths to allow '*connectors*' to be implemented.

Based on this organizational misalignment, DOL's IT Operations Group formally identified the existing FICAM investment as "*incapable of supporting the enterprise needs for FICAM*". Instead, the more immediate *Project level* concerns associated with *Cloud Email* were elevated as the Agency's highest concern. This determination was made as a direct result of management authorities whose job responsibilities require them to only focus on Operational needs. Unfortunately, it results in solution approaches that will curtail Enterprise considerations and yield higher TCO models over time, based on the resulting adoption of point-up/one-off solutions that are segregated from broader Enterprise concerns (e.g. FICAM). In accordance with best practices, these implementation approaches should be avoided when engaging Segment Architectures or strategic initiatives. As a result, considerations regarding *Identity Provider versus Service Provider* models are not understood and will likely lead to Agency risk for meeting the broader enterprise needs (e.g., establishing IT Modernization approaches capabilities). The results are demonstrative of the *Cart Before the Horse*.

Decision making at an IT Operations level introduces Agency budgetary risk for successful strategic accomplishment of FICAM. In this example, DOL's determination to redirect FICAM efforts and reengage in planning is one of inadequate scope and is not aligned at the correct management level within the Agency. Additionally, existing budgets from OMB Exhibit 300 submissions were redirected from their stated purpose, resulting in budget/funds misalignment as reported as part of OMB 300 Part A/B processes. The Agency also introduces significant risks under the Federal Acquisition Regulation (FAR) based on its redirection of funds from a best value Offeror for FICAM Systems Integration and redirecting those funds to another contractor/vendor within the organization which most certainly do not have 1) appropriate Contractual Scope to address the need 2) appropriate skill sets or Subject Matter Expertise to effectively meet enterprise need for FICAM or HSPD-12 related concerns, and 3) appropriate designations or certifications required to provide solutions related to HSPD-12 (e.g., GSA Schedule 70 SIN 132-62 or listing in www.idmanagement.gov as a Qualified Integrator).

Recently, only 6 months after removing the Best Value Offeror from the FICAM Program, this DOL Operations group came to the conclusion that FICAM was simply '*too difficult a problem to solve*'. This is representative of inadequate skills and experience being available to address this Federal strategic need. As of April 2013, an Agency internal determination was to put this mandated initiative '*on hold indefinitely*', while the American taxpayers' money along with active yet effective vendor Contracts continue to remain misaligned.

Lessons Learned

- Agencies should engage appropriate Management Sponsorship with FICAM Programs
- Ensure architecturally minded professionals with deep Subject Matter Expertise are involved in Cloud service adoption and who offer sufficient background and experience in HSPD-12 and FICAM to mitigate Agency risks
- Tackle Infrastructure dependencies as a separate underlying concern that is subordinate to broader Enterprise Service needs, inclusive of FICAM, Cloud Email, and other services

©2013 LS3, Incorporated.

- Secure Executive Sponsors that will govern solution migration, adoption, or implementation for high criticality Programs, ensuring appropriate budgets are allocated and that TCO and ROI models are realized
- Agencies that seek to engage in FICAM initiatives should ensure appropriate SMEs are available to support the planning, design, and implementation of these mandated solutions. As demonstrated by DOL, Agencies that 'strike out alone' to manage these efforts with existing or conveniently available staff are immediately set up for failure.

The Department of Veteran Affairs supports a long standing capability with its E-Authentication Project, which was subsequently re-branded to Veterans Affairs Authentication Federation Infrastructure (VAAFI). The technical offerings of this project have sought to expand within the Agency and to Federal Business Partners, engaging limited sets of technical capability (e.g., SAML Assertions) for managing Identity and Security lifecycles.

Unfortunately, VA does not have a comprehensive set of *Organizational Identity* data that can be used or applied in robust Enterprise IAM or FICAM solution implementation. Instead, VAAFI leverages *Identity* data provided from an external *Identity Provider*, most notably Department of Defense, which provides Veteran *Identity* data that VA can use. The most authoritative set of Internal User (i.e., Employee, Contractor, and Affiliated Person) data is the VA's HSPD-12 PIV System solution, which no longer shares any system interconnection or relationship with VA Enterprise IAM efforts[4]. Further, the VA Active Directory solution suffers from poor data management practices, resulting in low quality data of diminished to no value with regard to Enterprise IAM approaches or technical offerings.

The fundamental lack of *Organizational Identity* data, where VA manages its own *Identity* information as an *Identity Provider*, restricts VA investment from fully aligning with FICAM models. VA's approach omits major Service components that are architecturally required to address the full set of identity and security lifecycle management functions. Further, VA is not taking a top-down architectural approach to solution implementation(s). The capability to engage in *Federated Identity Management, Federated Authentication,* and other types of related services falls at the "*top of the IAM service pyramid*". That is to say that these capabilities are built up from architectural Service Models that serve as foundational elements within well-planned architecture. The VAAFI project-driven approach is a bottom-up approach that seeks to develop capability and then to market that capability in search of a business need.

VA's approach results in a high-cost[5] project-driven focus to Enterprise IAM that lacks fundamental Enterprise *Identity* data to permit robust FICAM related services and capabilities. Where VA seeks to engage Cloud services with the current VAAFI capability, the only supportable offering is *Federated Authentication* for a subset of the Identity population. This makes the VA approach and solution incomplete at best.

Lessons Learned

[4] VA made the decision to fully segregate Enterprise IAM from HSPD-12 solutions in 2009, where the integrated capability that aligned with FICAM Segment Architecture was split into separate efforts and separate investments.

[5] Budgets for VA's Programs exceed $40M per year (as per OMB public budget data), and to date have only satisfied the needs of a handful of Web-based applications, demonstrating no real ROI and high TCO for the investment

©2013 LS3, Incorporated.

- VA's project driven approach is misaligned not just in terms of organizational management support, but in terms of its approach and alignment with other Identity and Security Management needs
- VA does not serve as the Enterprise *Identity Provider*, thus curtailing value from any investments made in the current Enterprise IAM Program consisting, predominately of limited VAAFI technical service offerings
- VA is the poster child of "*Cart Before the Horse*", with its investment in Federations and its complete lack of underlying architectural Service components required to realize value in Enterprise IAM or FICAM.

The General Services Administration has published its own Lessons Learned for Agencies to review (http://www.gsa.gov/portal/getMediaData?mediaId=165391).

VENDOR QUALIFICATIONS

Any vendor that wants to succeed in the management, planning, sustainment, or operations of HSPD-12 (*as well as ICAM*) technical frameworks must be dedicated to engaging industry and keeping pace with the evolution or changes associated with these technologies.

The GSA has established a certification program that reviews capabilities of industry vendors, and which results in a certification in HSPD-12 capabilities across a number of service categories. This program was established as a result of Directives such as: *OMB M-05-24 Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* and *OMB M-06-18 Acquisition of Products and Services for Implementation of HSPD-12*.

Important to note with regard to certified vendors is the Service Category they are assigned, ensuring that a *Certified Systems Integration Services and Products* vendor is used for these efforts. This is because the other categories of service (e.g., *Activation and Finalization Services and Products, Card Management and Production Services and Products, Enrollment and Registration Services and Products, Systems Infrastructure Services and Products*) are not as directly applicable to the experience, capability, and talent needed to succeed with migration and transition efforts. The *Certified Systems Integration Services and Products* vendors are more apt to address the integration requirements, end-to-end solution expertise, and direct technical capabilities needed for migration success.

Federal acquisition rules and laws require the use of Qualified or Certified vendors to address HSPD-12 related work efforts. Agencies can opt to engage the GSA Schedule 70 within Special Item Number 132-62 to acquire these resources or at a minimum must utilize the certified labor as listed on the ID Management web site (www.idmanagement.gov) within the acquisition process.

White Paper Author

LS3 Technologies is an organization that has been dedicated to the advancement, use, and practical application of HSPD-12 and ICAM for more than a decade. We specialize in researching, reviewing, and assessing each of the component technologies that comprise ICAM and HSPD-2 solutions. We dedicated significant corporate resources to finding and retaining talented industry experts that share a similar interest in investing themselves in these technologies to offer best-in-class solutions for our customers. Our best-in-

©2013 LS3, Incorporated.

class service capabilities have addressed the solution design, development, integration, and operational sustainment needs of PIV and FICAM for a decade.

LS3 Technologies, a valued partner, minority woman-owned 8(a) certified and Small Disadvantaged Business, specializes in full lifecycle IT solutions. Clients benefit from our solid reputation for rapidly and successfully implementing best-in-class practices, processes, and systems. We strive to offer an accelerated return on our customers' time and investment. We carefully select each team member to ensure the resources each provides matches or exceeds expectations of our customers. Our teams of experienced critical thinkers are results-oriented people that cover the full spectrum of the IT industry, with specialized focus areas dedicated to success in individual tasks, yet integrated to keep their eyes on the end state desired. Our cross-functional management approach permits emphasis of strengths within each team member while ensuring a collaborative and inclusive atmosphere for achieving results and making progress.

©2013 LS3, Incorporated.