Department of Homeland Security

Response to Office of Management and Budget Memo M-16-19

Implementing DCOI: DHS Enterprise Computing Services (DHS ECS) Strategic Plan

Office of the Chief Information Officer
Department of Homeland Security

October 7, 2016

DHS Data Center Optimization Implementation Strategy 2016-2020

Contents

Message from the Chief Information Officer

The Department of Homeland Security (DHS) Data Center Optimization Implementation (DCOI) Enterprise Computing Services (ECS) Strategic Plan identifies the most effective ways for the department to capitalize on opportunities and benefits of Enterprise Computing Services (ECS) to accelerate IT delivery, efficiency, and innovation across the DHS enterprise. This strategic plan aligns to, and enables the goals and objectives outlined the DHS IT Strategic Plan 2015-2018 as well as FITARA objectives for IT reform.

The DHS Enterprise Computing Services (ECS) concept of converged infrastructure is the next generation of DHS enterprise data center services and represents a key change opportunity in the way that government thinks about and leverages IT to support daily mission and business operations as well as manages its acquisitions and procurement processes to optimize data center capabilities and resources. Adoption and implementation of multi-provider and commercially provisioned services are being rapidly accelerated with the maturing of Federal Cloud Computing Initiative, the Federal Risk and Authorization Management Program (FedRAMP), the recent mandates including the Federal Information Technology Reform Act (FITARA), and the Data Center Optimization Initiative (DCOI). Therefore, our DHS Data Center Optimization Implementation (DCOIm) Strategy goes beyond the DHS private cloud to also encompass use of multi-provider and commercially provisioned computing services in the department's enterprise computing environment through the execution of an "Open Market" strategy via the Enterprise Computing Services (ECS). Adoption and implementation of enterprise computing options will provide DHS with alternatives to increase secure information sharing and collaboration, enhance mission effectiveness, and reduce total cost of Information Technology ownership, operation and sustainment.

I look forward to working through the ambitious goals and objectives described in this strategy, especially the opportunity to modernize and improve the way in which the private and public sectors partners will leverage cloud computing to provide goods and services.

We will continuously seek to refine and mature the cloud computing approach and maintain open communications within all levels of the Department, other Federal Agencies and our Industry partners. Active participation and commitment of all DHS Components is critical to ensure consistency, optimize benefits, and achieve the goal of this strategy.

1. Executive Summary

The DHS ECS Optimization Strategy implements DCOI and establishes and communicates the Department's vision and approach for delivering a wide variety of enterprise computing capabilities to improve mission and business effectiveness, increase operational IT efficiencies while protecting DHS data and infrastructure. In the current political, economic, and technological landscape, IT is expected to provide extensive and ever-increasing capabilities while consuming fewer resources. As a result, the Department must transform the way in which it acquires, operates, and delivers IT capabilities in order to realize increased efficiency, effectiveness, and security.

The Department has begun this transformation by establishing various initiatives that are aimed at achieving improved efficiencies in IT service delivery. One of these initiatives is the DHS ECS. The DHS ECS is a key component to enable the Department to achieve DHS next generation computing service delivery goals. The DHS Chief Information Officer (CIO) is committed to accelerating the adoption of next generation computing options through the alignment with Department-wide efficiency initiatives such as Unity of Effort, OMB Data Center Optimization Initiative (DCOI), and Federal IT Acquisition Reform Act (FITARA).

2. Introduction [1]

DHS ECS represents both DHS' next generation contract and business approach to achieving massively scalable processing because of the need to support more users who are accessing more applications and resources on a consumption basis. DHS' approach to ECS will focus on the concept of converged infrastructure solutions to manage customer demand for more virtual technologies and more integration with cloud. DHS ECS converged infrastructure solutions will employ physical (converged infrastructure deployment) and virtual (appliance which aggregates distributed resources) forms. Based on customer needs, these can be a multi-rack ecosystem or even a smaller, node-based, architecture supporting a specific use case. DHS ECS will help combine

[1] Next-Generation Convergence is the Future of Cloud and Data Center, Data Center Knowledge, February 11, 2016, http://www.datacenterknowledge.com/archives/2016/02/11/future-of-cloud-and-data-center-next-gen-convergence/

critical resources into one logical management layer with fewer management points that the customer must navigate and greater levels of customer control over their critical resources.

While the concept of converged systems is not new, the major difference for DHS ECS will be our focus on major optimizations, management tools, and application program interface (API) integration points to create a converged ecosystem. DHS ECS will help define the next-generation convergence environment by redefining how organizations deploy cloud and data center solutions.

DHS ECS will accomplish converged infrastructure efficiencies in several ways.

- DHS ECS will allow both DHS data center leadership and customers to pursue integration with third-party and provisioned solutions. This can be monitoring, security, networking services, application management, cloud services, and more to facilitate integration with other (external) data center and cloud resources.
- DHS ECS will allow DHS data center leadership and customers to manage data center environmental variables for greater data center efficiency by removing older, isolated components and aggregating critical resources based on where the business is going internal and external to the data center and how IT will support these goals. DHS believes that the converged infrastructure approach will actually help with the overall data center footprint, power utilization, and even cooling efficiencies. Similarly, DHS will apply the concept of converged infrastructure solutions to segment user groups and applications and create greater opportunities for multi-tenancy.
- DHS ECS will allow for data center and business agility by allowing the DHS customer to provision and de-provision resources based on context, application, etc., and adapt to very quickly changing business dynamics. Ultimately, by being able to be truly agile and supporting more business use cases, DHS ECS will create real performance and cost advantages for DHS mission customers.
- DHS ECS will impact security design by allowing DHS data center leadership to aggregate resources, set very specific control and management policies, and even allow access to workloads based on user context to create controls over sensitive data points. From this converged architecture, DHS ECS will control where resources go and how they interact with cloud technologies. Because security against advanced persistent threats (APTs) is a priority, through converged infrastructure, DHS ECS will set strict multi-tenancy policies and manage access based on a number of granular administrative controls over these new levels of management, workload, and cloud integration

2.1 Background

In response to the call for IT reform in 2011, DHS immediately began planning its enterprise computing services business model and putting the foundation in place for these service, which focused primarily on data center consolidation and delivery of as-a-service capability in the DHS private cloud. DHS has made significant progress against that strategy however, advancement in the market place command the need for an updated strategy. This DHS Data Center Optimization Implementation Strategy lays out the path forward for the Department and Components to have access enterprise computing alternatives and the multi-provider provisioned service sources through the DHS Enterprise Data Centers (EDCs). This strategy in conjunction with an enterprise computing roadmap, governance model, migration plans, and strategic communications will allow DHS to

realize the vision and goals set out in the IT Strategic Plan. This strategy puts in context OMBs Data Center Optimization Initiative. Simply stated ***it requires agencies to consolidate inefficient infrastructure, optimize existing facilities, improve security posture, achieve cost savings, and transition to more efficient infrastructure, such as cloud services and inter-agency shared services.***

2.2 Alignment to Business Goals

The DHS Strategic Plan, Fiscal years 2014-2018, focuses on how the department will implement the goals laid out in the 2014 Quadrennial Homeland Security Review (QHSR). The DHS Data Center Optimization Implementation Strategy supports and enables all of the DHS mission goals and objectives by providing alternative computing platforms that can scale to meet increased demand of mission operations in a secure and flexible manner. The Department has established a strategic sourcing initiative to provide Components access to service providers in the open market. This enables Components to be proactive in supporting the mission needs of their operators in scalable, yet secure and cost effective manner.

2.3 Data Center Ecosystem

The data center ecosystem establishes an environment where consumers and providers are connected via reliable networks to ensure full range of computing availability, accessibility, and reliability. This ecosystem operates by grouping multiple information technology (IT) components into a single, optimized computing package through converged infrastructure. The following excerpt and references from Wikipedia provide some insight into the impact of converged infrastructure.

> *"Writing in CIO magazine, Forrester Research analyst Robert Whiteley noted that converged infrastructures, combining server, storage, and networks into a single framework, help to transform the economics [of] running the datacenter thus accelerating the transition*

to IP storage to help build infrastructures that are "cloud-ready".[2] The combination of storage and compute into a single entity is known as converged storage.[3]

In April 2012, the open source analyst firm Wikibon released the first market forecast for converged infrastructure,[4] with a projected $402B total available market (TAM) by 2017 of which, nearly two thirds of the infrastructure that supports enterprise applications will be packaged in some type of converged solution by 2017.

InformationWeek[5] highlighted the promise of two long-term advantages of a unified data center infrastructure:

1. *Lower costs as the result of both:*
    1. *lower capital expenses resulting from higher utilization, less cabling, and fewer network connections*
    2. *lower operating costs resulting from reduced labor via automated data center management and a consolidating storage and network management infrastructure teams*
2. *Increased IT agility by:*
    1. *virtualizing IP and Fibre Channel storage networking*
    2. *allowing for single console management.*

Data centers around the world are reaching limits in power, cooling and space.[101] At the same time, capital constraints are requiring organizations to rethink data center strategy. Converged infrastructure offers a solution to these challenges."

---

[2] Whiteley, Robert. Research. "Your Next IT Budget: 6 Ways to Support Business Growth," *CIO Magazine*, July 21, 2010

[3] Davis, Jessica. "Pivot3 Offers Converged Storage Platform to Data Protection Market," *ChannelInsider*, September 30, 2010

[4] Converged Infrastructure Takes the Market by Storm, Wikibon, August 12, 2012,, http://wikibon.org/wiki/v/Converged_Infrastructure_Takes_the_Market_by_Storm

[5] Crump, George. "Why 'Unified' Is The Hot New Idea For Data Centers," *InformationWeek*, March 14, 2009

3. Mandates

The Federal Government continues to accelerate the pace at which it will realize the value of DHS ECS alternatives by requiring agencies to evaluate safe, secure enterprise computing options before making any new IT investments. In alignment with Federal and Department-wide IT efficiency mandates, the DHS ECS model is committed to providing a secure, resilient, and fully optimized enterprise computing capabilities. Specific mandates include:

Specific mandates include:

Federal Information Technology Shared Services Strategy, May 2, 2012: [6] Provides organizations in the Executive Branch of the United States Federal Government (Federal Agencies) with policy guidance on the full range and lifecycle of intra- and inter-agency IT shared services that enable mission, administrative, and infrastructure-related IT functions.

Federal Information Technology Acquisition Reform Act (FITARA), 2015: [7] Provides the statutory basis for Federal-wide IT reform

Office of Management and Budget (OMB)-directed Data Center Optimization Initiative (DCOI), August 1, 2016: [8] Requires agencies to develop and report on data center strategies to consolidate inefficient infrastructure, optimize existing facilities, improve security posture, achieve cost savings, and transition to more efficient infrastructure, such as cloud services and inter-agency shared services.

Federal CIO 25 Point Implementation Plan to Reform Federal Information Technology Management, Dec 9, 2010: [9] Specifies that "Agencies must focus on consolidating existing data centers, reducing the need for infrastructure growth by implementing a Cloud First policy for services, and increasing the use of available cloud and shared services".

[6] https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/shared_services_strategy.pdf.
[7] Title VIII, Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, Pub. L. No. 113-291.
[8] Office of Management and Budget (OMB) Memorandum for Heads of Executive Departments and Agencies, M-16-19, Data Center Optimization Initiative (DCOI), August 1, 2016
[9] https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf

Federal Risk and Authorization Management Program (FedRAMP): [10] Provides joint "provisional" authorizations and continuous security monitoring services applicable to "Executive departments and agencies procuring commercial and non-commercial cloud services that are provided by information systems that support the operations and assets of the departments and agencies, including systems provided or managed by other departments or agencies, contractors, or other sources".

Federal Cloud Computing Strategy, Feb 8, 2011: [11] Intends to articulate the benefits, considerations, and trade-offs of cloud computing by: providing a decision framework and case examples to support agencies in migrating towards cloud computing; highlighting cloud computing implementation resources; and, identifying Federal Government activities and roles and responsibilities for catalyzing cloud adoption.

Pending legislation includes:

Cloud Infrastructure Transition Act or Cloud IT Act: [12]Promote innovation and realize the efficiency gains and economic benefits of on-demand computing by accelerating the acquisition and deployment of innovative technology and computing resources throughout the Federal Government.

4. Guiding Principles

The guiding principles associated with DHS ECS are precepts, rules or fundamental ideas that provide overall direction to components, program managers and/or application owners. The following principles embody the key ideas that shaped the development of the DHS Data Center Optimization Implementation Strategy and will continue to guide decisions during its implementation.

- **Mission effectiveness** – DHS must ensure that it does not compromise its mission by unrealistically trading the confidentiality, integrity and availability of critical data and information in pursuit of the benefits the enterprise services may offer. The potential

[10] https://www.fedramp.gov/about-us/about/
[11] https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf
[12] HEN15F65, Discussion draft for proposed legislation

technology vulnerabilities and impacts to operations must be continuously assessed and then weighed against the advantages of adopting DHS ECS enabling capabilities.

- **Common standards** – The design and use of the enterprise computing model will follow approved Homeland Security (HLS) architecture standards and operational directives to ensure the maximum level of interoperability across multiple hosting environments. This ensures that DHS applications and data are modernized and optimized providing maximum interoperability with other DHS components and homeland security partners.
- **Resilient and secure** – Dynamic security requires the continuous monitoring and evaluation of systems, capabilities, interfaces, applications and data transactions to assess threats to cybersecurity and risks that may affect confidentiality, integrity and availability. Security countermeasures are integrated from the beginning, protecting critical data to ensure that users and applications access only the data for which they are authorized.
- **Service level management** –Service level management and service level agreements are well defined in the planning stages that include explicit service level agreements (SLAs) for security, continuity of operations, and service quality and address mutual management processes, periodic reporting, and quality assessments.
- **Minimization of redundant data sources** – The use and reuse of defined authoritative data sources and standard data services provide access to cost-effective structured and unstructured data through simplified interfaces. Improved data quality is achieved by performing functions such as eliminating duplication, consolidation and tagging of all data in DHS ECS environments.
- **Interoperability & portability** – Compliance with DHS data and information sharing standards to ensure interoperability of applications and data for effective information sharing among component's and homeland security partners. This principle ensures that DHS information is able to move seamlessly between infrastructure workloads and multi-vendor providers to provide a common user experience.

5. Strategic Approach

As stated in the DHS IT Strategic Plan 2015-2018, DHS IT enables secure resilient capabilities to achieve interoperability, information sharing, and unity of effort for DHS and its partners. DHS ECS computing, when coupled with the appropriate applications and infrastructure, will enable authorized users to harness the power of the multi-provider and commercial services to unify national efforts to prevent and deter terrorist attacks; and protect against and respond to threats and hazards to the Homeland.

DHS ECS will expedite the transformation of many remaining legacy IT business models from an asset based culture into a services based, customer-centric IT business model; providing operational expenditure transparency, reduction in capital expenditures and reduced time to market for new capabilities. To accelerate this transformation, DHS will continue initiatives already associated with DHS optimization efforts as well as leverage new approaches.

- DHS will continue strengthening the foundation by focusing on improving network security and throughput of DHS OneNet to ensure that sufficient capacity exists for the business community to access and securely work using commercial DHS ECS capabilities.

- DHS will continue emphasis on the rationalization of existing systems, applications and associated data (i.e., the use of authoritative data sources) while determining the most appropriate deployment model for migration and improving secure mobile computing capabilities.
- DHS will continue to capitalize on the FedRAMP and DHS-approved service providers to the extent that doing so aligns with mission requirements without compromising security.
- In order to reduce the amount of contracting lead time, shorten implementation timelines, and effectively keep pace with the emerging market; DHS has established the ECS framework to build upon the current Enterprise Data Center (EDC) capabilities. The DHS ECS expands enterprise capabilities by providing access to multi-provider and commercial, as well as DHS-owned, services through the EDC that are shared, on demand, and take advance of Public, Private, Hybrid, Community, as well as IaaS, PaaS, SaaS). DHS will utilize the ECS framework as a holistic and enterprise approach to promote the use of approved DHS ECS providers. The ECS framework identifies the people, processes, and tools necessary to facilitate the appropriate decisions for selecting the path for provisioning the required infrastructure computing services. Figure 1 illustrates the upfront decisions that need to be considered when leveraging the ECS framework.

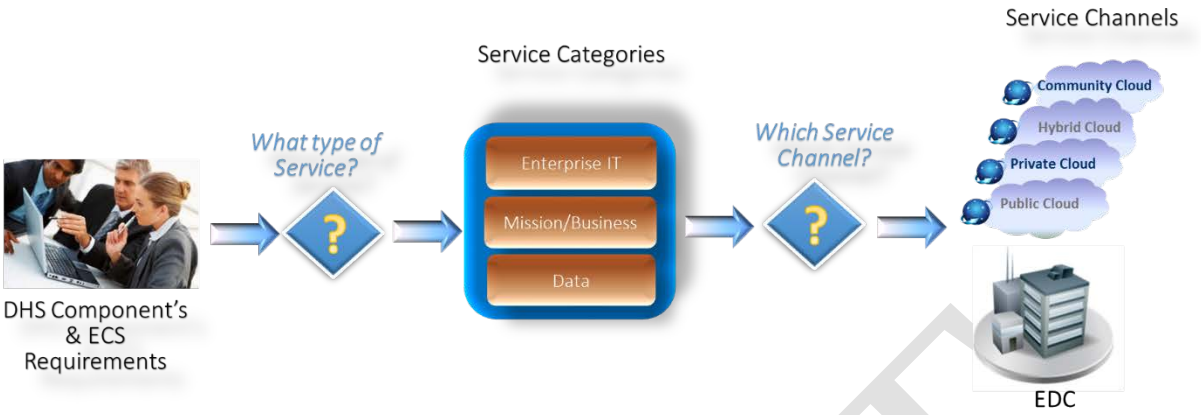

Figure 1: DHS Enterprise Computing Services Overview

DHS' strategy will ensure that there will be IT service options that are aligned to the business needs of DHS IT and Non-IT programs. To accomplish this, DHS will apply the repeatable process of the Service Management Framework and governance to implement, manage, and support on-demand access to a shared pool of internet-based computing resources[13] that can be provisioned rapidly and released with minimal management effort and zero loss of productivity to ensure customer requirements are being met consistently. DHS' strategy will ensure that prospective service providers that are external (to DHS) have a demonstrably proven performance record and meet all DHS compliance, privacy, and security requirements. Our strategy will ensure that existing and prospective service providers that are internal (to DHS) have conducted a comprehensive business analysis to establish that the requirement cannot be met by existing private or public applications, services, and models; constructed a well-documented business case; sourced the service provider(s); and planned, procured, implemented, and assessed the continued quality and performance of the solution. Finally, DHS' strategy will ensure technical and managerial support to the Program Manager in evaluating the potential for enterprise computer service solutions to deliver improved

[13] For example, networks, servers, storage, applications and services

mission (or business) performance at a lower cost through internet-based data integration, scalability, control, and security.

Due to the wide variety of architectures, configuration items, services, deployment models, and technologies that must coexist and operate homogeneously, the DHS will only implement and initialize service management processes, procedures, and architecture that:

- Provides policies and process assets (e.g. guides, process descriptions, templates, standards, samples), based on industry practices, to establish a defined and repeatable approach;
- Identifies all of the processes, methods, functions, roles and activities that are used to enable the delivery of services to customers;
- Enables a greater understanding of services, their value to their customers; ensure services facilitate desired outcomes, within the agreed to costs, and minimize risks;
- Provides strategic direction and assessments of Enterprise Services that support the core business, improve functionality, support acquisitions efforts, and ensure services deliver value to customers.
- Communicates and report on the value of services on IT Operations internally and externally to the Department; and,
- Provides subject matter expert (SME) support to DHS service provider that lack required expertise in service delivery; provide good repeatable practices to create effective service.

These efforts will strengthen DHS' ability to acquire multi-vendor and commercial enterprise computing services that are secure, governed, and offer efficiency gains that are currently lacking in today's IT environment. In order for the Department to gain maximum efficiency gains ECS, DHS will leverage and develop define roadmaps to guide its path towards the optimization targets established by OMB.[14] The Departmental approach will be based on developing a 3 year forecast that outlines the procurement of DHS ECS aligned to the annual planning cycle. DHS will utilize an approach for constructing its roadmap for DHS ESC optimization targets that is based on developing an inventory of the enterprise-wide IT systems owned, operated, or maintained by or on behalf of the DHS. The Department will leverage its road mapping activities to assess whether the system is suitable for transition to DHS ECS optimization targets, a timeline for migration to the target

[14] Ibid no. 8

computing environment, and specific benchmarks that can be achieved by specific dates; and year-by-year calculations of investment and cost savings.

5.1 Service Governance and Management

DHS ECS governance strategy will focus on instituting Service Management business practices that are core to services governance. Enhanced governance processes and policy enforcement mechanisms will be instituted by the DHS CIO and implemented by the Data Center Division (DCD) of the Information Technology Services Office (ITSO) to manage the rapid evolution of ECS within the Department, maximizing the potential value of IT service delivery and minimizing the risks. This strong governance mechanism will support consistent interpretation of policy, monitor DHS enterprise computing performance, and address consumer and provider issues. Service governance will ensure alignment of DHS investments, policies, processes and standards to enable achievement of DHS ECS optimization targets. The Department will exercise all governance mechanisms to ensure ECS options are analyzed during the budget and acquisition processes for each Program and/or investment.

To support the service governance process, DHS has established and manages an enterprise computing service lifecycle that defines the applicable activities necessary to identify, select, design, deploy, and deliver ECS services within the DHS environment. The enterprise computing services lifecycle is embedded into the DHS Systems Engineering Lifecycle (SELC) to guide and align IT service related decisions. The enterprise computing service lifecycle serves as means to determine best value between alternatives, defining a service investment management process that enables the rapid evolution of DHS ECS optimization goals and prevents non-standards-based IT service silos from proliferating within the enterprise.

DHS governance and service level management will address the ten unique areas of focus that were jointly identified by the Federal CIO and the Federal Chief Acquisition Officers Councils as

requiring the most attention when bringing together the relevant agency stakeholders to more effectively procure, govern and manage IT as a service. [15]

Selecting a DHS Enterprise Computing Service: Choosing the computing service model is the first step in this analysis as well as the first step in governance. The Administration's "Cloud First" and "Shared First" policies dictate that an agency must default to using a cloud computing solution if a safe and secure one exists. "Each service model offers unique functionality depending on the class of user, with control of the environment decreasing as you move from Infrastructure to Platform to Software. Infrastructure is most suitable for users like network administrators as agencies can place unique platforms and software on the infrastructure being consumed. Platform is most suitable for users like server or system administrators in development and deployment activities. Software is most appropriate for end users since all functionalities are usually offered out of the box. Understanding the degree of functionality and what users in an agency will consume the services is critical [to DHS' ECS strategy] in determining the appropriate cloud service to procure." [16]

Selecting a DHS ECS-Approved Cloud Deployment Model - NIST defines four deployment models for cloud services:[17] These service deployments include private, public, community, and hybrid and are defined by NIST.[18] "These deployment models determine the number of consumers (multi-tenancy), and the nature of other consumers' data that may be present in a cloud environment. A public cloud does not allow a consumer to know or control who the other consumers of a cloud service provider's environment are. However, a private cloud can allow for ultimate control in selecting who has access to a cloud environment. Community clouds and Hybrid clouds allow for a mixed degree of control and knowledge of other consumers. Additionally, the

[15] Creating Effective Cloud Computing Contracts for the Federal Government, Best Practices for Acquiring IT as a Service, a Joint Publication of the Federal CIO Council and the Chief Acquisition Officers Council, in coordination with the Federal Cloud Compliance Committee, page 4, February 24, 2012

[16] Ibid 14, page 5

[17] See NIST Special Publication 800-145.

[18] The NIST Definition of Cloud Computing: recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-145, September 2011

cost for cloud services typically increases as the control over other consumers and knowledge of these consumers increases. When consuming cloud services, [DHS strategy will focus on understanding] what type of government data they will be placing in the environment, and select the deployment type that corresponds to the appropriate level of control and data sensitivity." [19]

Service Providers and Terms of Service Agreements: DHS ECS governance will enforce common acceptable use standards across all users to effectively maintain how a consumer uses a service provider environment. This will include the publication and oversight of policies regarding Terms of Service Agreements (TOS) and Non-Disclosure Agreements (NDAs) to enforce acceptable Service Provider personnel behavior when dealing with Federal data. TOS and NDAs need to be fully contemplated and agreed upon by both Service Providers and DHS Program Managers to ensure that all parties fully understand the breadth and scope of their duties when using enterprise computing services.

Service Level Agreements (SLAs): DHS ECS governance will enforce use of DHS templates and guidelines for Service Level Agreements (SLAs) under the overall computing contract between a Service Provider and a DHS Program Manager. DHS governance activities will include advice and support to Program Managers in defining acceptable service levels to be provided by the Service Provider to its customers in measurable terms. Service Provider performance will clearly specified in all SLAs and all SLAs will be fully incorporated, either by full text or by reference, into the Service Provider contract

Service Provider, Agency, and Integrator Roles and Responsibilities: DHS ECS governance will ensure the effective guidance for the procurement of services for system integrators and/or service/system resellers under subcontracts or separate contracts from the service contract. This governance and guidance will apply in those instances in which integrators can provide a level of expertise within Service Provider environments that Programs may not have, thus making transition to the DHS ECS framework easier. DHS governance oversight will focus on clearly defining scenarios, roles and responsibilities to enhance the end-user's ability to fully realize the benefits of the enterprise computing system or service.

[19] Ibid 14, pages 5-6

Standards: When Federal agencies procure enterprise computing solutions, U.S. laws and associated policy require the use of international, voluntary consensus standards except where inconsistent with law or otherwise impractical.[20] DHS ECS governance will focus on leveraging the guidance of Standards Developing Organizations (SDOs) such as the National Institutes of Standards and Technology (NIST) in all DHS application of conceptual models, reference architectures, and standards to facilitate communication, data exchange, and security for enterprise computing functions, requirements, and roadmaps. DHS will particularly promote publications that address security, interoperability, and portability.[21] Required standards publications include NIST Special Publication 500-291, NIST Cloud Computing Roadmap, presents these standards in the context of the NIST Cloud Computing Reference Architecture using the NIST taxonomy in NIST Special Publication 500-292, NIST Cloud Computing Reference Architecture.

In considering DHS ECS solutions, all DHS Programs will ensure availability of technically sound and timely standards to support their missions.[22]

- Standards specification: In accordance with Office of Management and Budget (OMB) Circular A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities, Programs will specify relevant voluntary consensus standards in their procurements. The NIST Standards.gov website includes a useful list of questions that agencies should consider before selecting standards for agency use15.
- Standards requirements: Programs will contribute clear and comprehensive mission requirements to help support the definition of performance-based computing standards by the private sector16.

[20] Trade Agreements Act of 1979, as amended (TAA), the National Technology Transfer and Advancement Act (NTTAA), and the Office of Management and Budget (OMB) Circular A-119 Revised: Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities

[21] Special Publication 500-291, NIST Cloud Computing Standards Roadmap, lists relevant standards for security (see Table 5), interoperability (see Table 6), and portability (see Table 7).

[22] Ibid 14, page 11

Enterprise Computing Reference Architecture: DHS ECS will work with Program Managers to ensure that service providers categorize their ECS cloud access service using the NIST Cloud Computing Reference Architecture. This can be accomplished by the vendor's "mapping" of services to the reference architecture, and presenting this "mapping" along with the vendor's customized marketing and technical information. The reference architecture mapping provides a common and consistent frame of reference to compare vendor offerings when evaluating and procuring cloud services.

IPv6: The Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council issued a final rule in December 2009 amending the Federal Acquisition Regulation (FAR) to require all new information technology acquisitions using Internet Protocol (IP) to include IPv6 requirements expressed using the USGv6 Profile and to require vendors to document their compliance with those requirements through the USGv6 Testing Program. Accordingly, DHS Programs will include language in solicitations and contracts, where applicable to DHS ECS solutions.

Security: Placing agency data on an information system involves risk, so all DHS Programs must ensure that the IT environment in which they are storing and accessing data is secure. As such, all IT systems used by DHS Programs must meet the requirements of the Federal Information Security and Management Act (FISMA) and related agency-specific policies. FISMA requires that all systems undergo a formal security authorization which details the Service Provider's responsibilities for implementation and continuous monitoring of security controls; effective monitoring for incidents and threats to ensure compliance;[23] key management[24] to include how the key's encrypted data are escrowed and what terms and conditions of escrow apply to accessing encrypted data; adequate controls and appropriate tools to conduct forensics of the Service Provider's environment; implementation of two-factor authentication to gain access to a Service Provider's environment; and authorized access,

[23] Compliance requirements apply to all data security standards, laws, initiatives, and policies including FISMA, the Trusted Internet Connection (TIC) Initiative, ISO 27001, NIST standards, and agency specific policies.

[24] Also known as fair cryptosystem and key escrow both of which refer to an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that an authorized third-party may gain access to the keys in certain documented circumstances.

management and preservation of transaction records and audit logs. [25] After the Service Provider's environment has gone through a security authorization, the DHS ECS governance requires that the Program Manager review the risks posed by placing Federal data in that system, and if this risk level is acceptable, may seek an authority to operate (ATO).Continuous Monitoring: DHS Programs must continue to ensure a Service Provider environment maintains an acceptable level of risk. In order to do this, DHS ECS governance requires that Program Managers work with Service Providers to implement a continuous monitoring program[26] to ensure that the level of security through a Service Provider's initial security authorization is maintained while Federal data resides within a Service Provider's environment. Such continuous monitoring programs must be developed in accordance with the NIST Publication 800-137 framework and Department of Homeland Security (DHS) guidance, detailed contractually, and must at a minimum address updates to the authorization based on any significant changes to a CSP environment, address new FISMA requirements, and provide updates to control implementations on a basis frequent enough to make on-going risk based decisions. [27]

- FedRAMP: On December 8, 2011, OMB released a policy memo addressing the security authorization process for cloud computing services. Specifically, this memo requires all Federal agencies to use the Federal Risk and Authorization Management Program (FedRAMP) when procuring and subsequently authorizing cloud computing solutions. [28]Specifically, DHS cloud computing governance required Program Managers to:
    - Use FedRAMP when authorizing cloud services;
    - Use the FedRAMP process and security requirements as a baseline for authorizing cloud services;
    - Require CSPs to comply with FedRAMP security requirements;

[25] NIST Special Publication 800-53.

[26] DHS' National Cyber Security Division memo: "FY 2011 Chief Information Officer Federal Information Security Management Act Reporting Metrics."

[27] Ibid 14, page13.

[28] Ibid 14, page 12.

- Establish a continuous monitoring program for cloud services;
- Ensure that maintenance of FedRAMP security authorization requirements is addressed contractually;
- Require that Cloud Service Providers route their traffic through a Trusted Internet Connection (TIC); and
- Provide an annual list of all systems that do not meet FedRAMP requirements to OMB. DHS governance of this process will notify Program Managers when to provide this list to the DHS CIO EBMO by system through their Application Services Council (ASC) Member.

Privacy: Federal agencies and employees can be subject to both criminal and civil penalties for misuse and erroneous disclosures of data that contains protected information, even when this data is in a Service Provider environment. Personal information, and specifically Personally Identifiable Information (PII), can relate to information about Federal agency employees, other internal users, and a broad array of individual members of the public and can be found in email, agency reports, memos, or even web pages.[29] DHS ECS governance of privacy in the cloud requires that Program Managers collaborate and consult with legal counsel and privacy offices to obtain advice and guidance on particular laws and regulations when data they place in a Service Provider environment will contain PII.

Five areas identified as key factors for Program Managers to consider when PII is or could be a part of the data moved to a DHS ECS cloud environment are: compliance with the Privacy Act of 1974 and related PII requirements, privacy impact assessments (PIAs), privacy training, data location, and how a Service Provider responds to a breach. How a Service Provider addresses privacy concerns within their environment may impact the overall price and technical structure for a proposed

[29] Under OMB guidance, PII is broadly defined as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." Available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.

solution, so Programs are advised to gather privacy requirements as early as possible in order to fully understand how a Service Provider will enable an agency to maintain its duty to protect PII. [30]

E-Discovery: E-discovery has the potential to be vastly more expensive due to the sheer volume of ESI that Federal agencies generate and are required to maintain. These costs result from not only the inefficient use of agency IT and legal resources to preserve, search, collect, and produce ESI, but may result from court sanctions for noncompliance with e-discovery obligations.[31] Given the inevitability of agency litigation and the potential costs and benefits of moving and storing data in a Service Provider environment, DHS ECS governance of cloud computing requires Program Managers to have documented discovery process for locating, preserving, collecting, processing, reviewing and producing electronically stored information (ESI) in the context of civil litigation or investigation;[32] based in established rules of civil procedure; [33] and available not only when litigation has commenced but when it is reasonably anticipated. [34]

Freedom of Information Act (FOIA): DHS' obligation to comply with the FOIA[35] does not change as an agency's IT system moves to a CSP environment. The FOIA generally provides that anyone may request agency records, including information that is maintained in electronic form or

---

[30] Ibid 14, pages 18-23.

[31] In Re Fannie Mae Securities, 552 F.3d 814 (D.C. Cir. 2009); see also Moore v. Napolitano, 2010 WL 2780914 (D.D.C. July 15, 2010) (upholding sanctions).

[32] The Sedona Conference Glossary (http://www.thesedonaconference.org/content/miscFiles/TSCGlossary_12_07.pdf) and the EDRM model (www.edrm.net). The Sedona Conference Glossary also contains many helpful definitions of common e-discovery terms and concepts (both legal and technical).

[33] E.g. Federal Rules of Civil Procedure: Rule 16 (Agreements/Scheduling Order); Rule 26(f) (Meet & Confer re ESI); Rule 26 (b) (2) (Inaccessible ESI); Rule 33 (ESI Interrogatories); Rule 34(a) (ESI New Category); and Rule 34(b) (Form ESI).

[34] See e.g. Micron Tech., Inc. v. Rambus Inc., 2011 WL 1815975 (Fed. Cir. May 13, 2011) ("the proper standard for determining when the duty to preserve documents attaches is the flexible one of reasonably foreseeable litigation…."); Zubulake v. UBS Warburg, 220 F.R.D. 212 (S.D.N.Y. 2003) ("Zubulake IV") (at the very start of a case or when litigation is reasonably anticipated, a litigation hold must be issued to prevent the spoliation of potential evidence).

[35] 5 U.S.C. 552(b). See DOJ Office of Information Policy web page for general guidance, at http://www.justice.gov/oip/oip-guidance.html.

in traditional paper files. Storing records in a cloud environment does not affect their agency record status.[36] Agencies are required to produce information in any form or format requested by the person if the record is readily reproducible by the agency in that format.[37] Cloud solutions present possibilities for efficiencies in DHS Program abilities to do robust enterprise searches for records responsive to FOIA requests. In order to ensure that DHS Programs have the ability to search and locate specific ESI required for a given FOIA request, DHS governance of cloud computing requires that Programs focus on search capabilities in the cloud. This may include considering specific software or the methods used for searching, or incorporating search and retrieval standards. Furthermore, Programs may consider whether a Cloud Service Provider should have the capability and tools to de-duplicate, de-conflict, thread, and redact paper documents, active files and backup archives, emails, and other electronic files in order to prepare for production material that is potentially responsive to a FOIA request since the DHS Program user might lose the ability to internally search and retrieve data in the cloud. [38]

E-Records: In November 2011, President Obama issued a Presidential Memorandum on "Managing Government Records" that expressly referenced agencies "deploying cloud based services or storage solutions" as part of their records management programs.[39] DHS' obligation to comply with the Federal Records Act (FRA)[40] does not change as an IT system moves to a Cloud Service Provider

[36] The FOIA, as amended by the OPEN Government Act of 2007, specifically includes within the definition of an agency record "any information . . . that is maintained for an agency by an entity under Government contract, for the purposes of records management." See 5 U.S.C. § 552(f) (2) (B) (2006 & Supp. III 2009).

[37] 5 U.S.C. 552(a) (3) (B).

[38] Ibid 14, page 29.

[39] The Presidential Memorandum directs the Archivist of the United States and the Director of OMB to issue a Records Management Directive containing specific steps in reforming and improving agency records management policies and practices. This Directive, when issued in mid-2012, will be informed by required agency reports devoted in part to describing how agencies are "deploying cloud based services or storage solutions." http://www.whitehouse.gov/the-press-office/2011/11/28/presidential-memorandummanaging-government-records.

[40] National Archives and Records Administration (NARA) Bulletin 2010-05, Guidance on Managing Records in Cloud Computing Environments, Sept. 8, 2010 ("Federal agencies are responsible for managing their records in accordance with NARA statutes including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B). This is true regardless of which cloud service and deployment models are adopted.

environment. What does change is the way DHS Programs can ensure that they maintain control over the management of and access to records covered under the FRA, including enforcing (through contractual provisions and otherwise) a fundamental understanding on the part of Cloud Service Providers regarding Federal agency obligations under these laws. To enable proactive records planning, DHS Components records officers must be included in Program records planning in the cloud early in the procurement cycle as well as in the subsequent transition to Cloud Service Provider environments to properly plan and account for storing, migrating, disposing and/or deleting records.

5.2 Reform IT Financial, Acquisition, & Contracting Policy & Practices

Existing policies and processes that were implemented to support traditional IT acquisition hamper today's delivery and operation of a Cloud-First approach. The Department's typical acquisition approach bases investment decisions on significant investigation of capability needs, requirements definition, analysis of alternatives (AoA), and system growth projections. This works in an environment with relatively fixed requirements, known future needs, and static technology, but does not accommodate a multi-provider cloud environment. The Department must alter this acquisition approach if it expects to keep pace with IT advancements and achieve the efficiencies these advancements represent. To accomplish this, the DHS ECS governance will work with Program, Procurement, and Budget stakeholders to:

- ***Streamline Key Processes to reduce Operations and Maintenance (O&M)*** costs by leveraging economies of scale, and automate monitoring and provisioning to reduce the human cost of service delivery and assurance.
- ***Change Acquisition and Contracting Models*** to reduce acquisition complexity; shift the mindset from acquiring and managing IT assets (materiel solution development) to providing and consuming services; and support new funding, contracting, and acquisition models for agile solutions.
- ***Publish Guidance and Policies*** that support transition to, and use of, cloud services.

However, NARA recognizes that the differences between models affect how and by whom (agency/contractor) records management activities can be performed.").

The Enterprise IT Service Management Directive establishes the delegation authorities for IT executives as well as the approval of cloud services throughout the Department and will guide stakeholders in collaborating on the policy and process reforms.

5.3 Implement a DHS ECS Outreach and Awareness Campaign

An impediment to the successful adoption of DHS ECS is not just technological in nature, but rather, there are cultural roadblocks that make it difficult for the Department's IT community to adopt a new technology and business model. As with any significant change, the move to the DHS ECS framework requires a shift in mindset to accept new ways of delivering solutions and an informed workforce to enable acceptance and use of IT services. Implementing a DHS ECS outreach and awareness campaign is essential to gather input from major stakeholders, expand the base of consumers and providers, and increase visibility of available service offerings throughout the Department. DHS is committed to working with Component stakeholders to implement an outreach and awareness campaign to expand the base of consumers and providers, and increase the visibility of available services in other parts of the Government. The Department will leverage the service management framework to inform the stakeholders on the key benefits and challenges of the ECS framework, including value propositions, security features and challenges, sample mitigation strategies, training, lessons learned, and case studies. This outreach will include:

- Identifying best practices to guide stakeholders in the adoption and implementation of DHS ECS, including the acquisition and provisioning process and identifying and evaluating associated compliance and legal issues;
- Establishing methodologies to enable effective assessment and implementation of DHS ECS, including consideration of maturity, cost recovery, security compliance, etc.;
- Identifying challenges and recommending mitigations to resolve them; and,
- Establishing metrics and associated performance measures demonstrating successful migrations to, and continued service quality, of DHS ECS.

Adopting DHS ECS will reduce acquisition and maintenance of dedicated, program-specific resources. The desired outcome is the transformation that will yield higher flexibility, lower costs, and improved quality of service through effective governance, reformed financial, acquisition, and contracting, and improved communications.

5.4 Optimize the Delivery of Secure Multi-provider Services

As stated in the DHS IT Strategic Plan Goal 3 the Department seeks to establish a model for continuous process improvement that enables transparent data driven decisions and rapidly deliver high quality IT capabilities. Additionally, Goal 4 seeks to empower DHS and its partners to operate secure IT systems and networks, keeping ahead of evolving cyber threats. The Department is responsible for the service architecture and standards that guide and inform how cloud computing technologies are designed, operated, and consumed within the DHS enterprise. The vision for the Department is a multi-provider enterprise computing environment that meets DHS IT objectives. Program managers and application/service owners will not need to design the physical infrastructure that hosts and runs their software applications. Instead, they will be responsible for deploying applications and services that conform to the established service architecture standards

To meet the objectives identified above, the DHS ECS architecture standards will need to evolve in order to extend the full range of IT services. The NIST Cloud Computing Reference Architecture and the NIST Cloud Computing Standards Roadmap will guide the Departments approach to cloud. Leveraging the NIST guidance, the Department will develop a series of relevant DHS reference architectures to guide the development of technical and solution architectures to influence/facilitate the delivery and adoption of DHS ECS capabilities.

In order to optimize the delivery of secure multi-provider DHS ECS, the department is adopting and implementing a limited set of standardized authentication, access management, and information sharing services that will enable effective management as an enterprise with a reduced intrusion surface for cyber threats. Some of these capabilities:

- Ensuring compliance with DHS Cyber requirements for encryption and key management integration with DHS's emerging ICAM services.
- Enabling integrated cyber intrusion detection and response.
- Providing integrated identity and access management controls and integration with DHS's emerging ICAM services
- Maintaining configuration baseline of DHS resources deployed into the cloud
- Enabling continuous monitoring and reporting on performance SLAs and Cyber controls

Data as a Service (DaaS)

Because of the huge impact that cloud computing can deliver to improve DHS data and information management, the DHS ECS diverges from NIST cloud services model definitions to uniquely identify DaaS. DHS ECS DaaS encompasses two primary activities. The first is the continued implementation of the DHS Data Strategy and deployment of standardized data interfaces that make DHS information visible and accessible to all authorized users. The second is the incorporation of emerging "big data" technologies and approaches to effectively manage rapidly increasing amounts of information and deliver new insights and actionable information. As the volumes of unstructured and structured data sets proliferate, our ability to capture and effectively process this information has not kept pace using traditional data management technologies. DHS ECS DaaS technologies and parallel computing clusters provide new capabilities to manage large, diverse data sets, enable new data transformation methods and enable advanced analytics.

5.5 Guide the Transition to DHS ECS

The Department will build on its enterprise services efforts and continue to deliver cloud services that provided improved IT capabilities at reduced costs. Components are encouraged to use Enterprise Services, Shared Services, and commercial vendors that meet their specific mission requirements. That being said there are a number of potential approaches to cloud-based service adoption each of which triggers different responses and results.

In order to ensure that cloud adoption and migration is a repeatable and predictable process the department will develop a DHS ECS Guide as a reference framework to guide project teams to minimize risk and maximize value. The DHS ECS Guide sets out the steps necessary for to migrate workloads to a cloud-computing environment.

Governance, architectural, technical and funding challenges become increasing magnified while deploying cloud solutions in an enterprise as large and complex as DHS. Ensuring that DHS mission needs are met and enhanced hinges on having a solid yet flexible strategy that informs trade space decision making and an architecture that addresses unique operational requirements.

6. Measuring the Benefits

"Governance" is the strategic task of setting the organization's goals and direction, specifying limitations, and establishing an accountability framework. In contrast, "management" is the allocation of resources and overseeing day-to-day operations of the organization. As the department begins to execute the strategy through governance, evolving OMB PortfolioStat data collection and reporting requirements will guide decisions to measure, monitor, and report the scale of adoption to identify progress towards the realized benefits. At a minimum, Programs incorporating cloud computing solutions into their systems and services will ensure they have incorporated methods and tools to measure progress in the following PortfolioStat focus areas.

- Standardized Cost Savings within the Programs IT Portfolio: DHS governance will communicate the level(s) (i.e., investment, program, project, application, system) at which Programs will establish data collections to address savings and cost avoidance due to transition to DHS ECS solutions and services. Programs will use the definitions provided in OMB guidance[41] to identify appropriate supporting data as well as regularly collect, track and report both realized and projected cost savings and cost avoidance. Programs will include explanations and justifications of success or failure to achieve projected savings goals as a factor in presentation of IT budget requests, as an indicator of delivering value, as a factor in root cause analyses, and as a prerequisite to be evaluated prior to acquisition review and approval.

[41] OMB Memorandum to the Heads of Executive Departments and Establishments, Circular No. A-131 (Revised), Value Engineering, December 25, 2013, in which cost savings is defined as a reduction in actual expenditures below the projected level of costs to achieve a specific objective and cost avoidance is defined as an action taken in the immediate time frame that will decrease costs in the future.

- Performance Indicators: Programs will identify measurable indicators of cloud computing solutions and services performance which will be subject to DHS PortfolioStat leadership review and approval. Programs will include explanations and justification of success or failure to achieve performance goals as a factor in presentation of IT budget requests, as an indicator of delivering value, as a factor in root cause analyses, and as a prerequisite to be evaluated prior to acquisition review and approval.
    - The following Key Performance Indicators (KPIs) will be used to control and measure aspects of DHS ECS service integration, delivery, and service adoption. As the department progresses towards DHS ECS goals it may add and/or adjust the KPIs. The KPI framework will describe a KPI statement, calculation, suggested targets, if within targets, and if below targets.
        - Service Availability
        - The speed/timeliness of execution
        - Accuracy of Service Execution
        - Legal/regulatory compliance of service output(s)
        - Cost of service execution
        - Subscriber satisfaction
        - Service execution business ratio
        - Workforce development in the context of cloud-based services
- Project Delivery Indicators: Programs will maintain accurate and up to date CPIC reporting of project delivery relative to available budgets and projected schedules. Programs will include explanations and justification of success or failure to achieve project delivery on budget and on schedule as a factor in presentation of IT budget requests, as an indicator of delivering value, as a factor in root cause analyses, and as a prerequisite to be evaluated prior to acquisition review and approval.
- World Class Customer Service: Programs will ensure that measurable indicators of the success or failure of customer service are maintained and available to be reported at all times. Programs will include explanations and justification of customer service success or failure as a factor in presentation of IT budget requests, as an indicator of delivering value, as a factor in root cause analyses, and as a prerequisite to be evaluated prior to acquisition review and approval.
- Alignment of Enterprise Computing Methods/Sources to the Long Term Mission of the IT Portfolio - Programs will align measurable indicators of enterprise computing solutions and services performance to the long term Portfolio mission. Programs will include explanations and justification of success or failure of this alignment to improve the long term mission as a factor in presentation of IT budget requests, as an indicator of delivering value, as a factor in root cause analyses, and as a prerequisite to be evaluated prior to acquisition review and approval.
- Shared Service Delivery – Programs will identify shared services spending in all IT budgets and uniquely identify such spending for enterprise computing solutions and services.

Programs will include explanations and justification of success or failure shared service delivery as a factor in presentation of IT budget requests, as an indicator of delivering value, as a factor in root cause analyses, and as a prerequisite to be evaluated prior to acquisition review and approval.

- Potential Duplication and Waste – Programs will flag indicators of potential or actual duplication and waste if they fail to achieve projected savings, performance, and/or shared service delivery goals. Programs will include explanations of duplication and waste as a factor in presentation of IT budget requests, as an indicator of delivering value, as a factor in root cause analyses, and as a prerequisite to be evaluated prior to acquisition review and approval.
- Federal Data Center Optimization Initiative (DCOI) – Programs will report quarterly to the DHS EBMO PortfolioStat Lead regarding DCOI metrics. Programs will include DCOI metrics in presentation of IT budget requests, as an indicator of delivering value, as a factor in root cause analyses, and as a prerequisite to be evaluated prior to acquisition review and approval.
- Federal Strategic Sourcing Initiatives (FSSI) – Programs will report quarterly to the DHS EBMO PortfolioStat Lead regarding compliance with FSSI. Programs will include FSSI compliance and transition status in presentation of IT budget requests, as an indicator of delivering value, as a factor in root cause analyses, and as a prerequisite to be evaluated prior to acquisition review and approval.
- Commodity IT – Programs will report quarterly to the DHS EBMO PortfolioStat Lead on commodity IT spending within their IT Portfolio. Programs will include commodity IT spending in presentation of IT budget requests, as an indicator of delivering value, as a factor in root cause analyses, and as a prerequisite to be evaluated prior to acquisition review and approval.
- Enterprise Cloud Services (ECS) Contract – Programs will report quarterly to the DHS EBMO PortfolioStat Lead regarding ECS spending within their IT Portfolio. Programs will include ECS spending in presentation of IT budget requests, as an indicator of delivering value, as a factor in root cause analyses, and as a prerequisite to be evaluated prior to acquisition review and approval.
- Cyber Security – Programs will report quarterly to the DHS EBMO PortfolioStat Lead on cyber security spending within their IT Portfolio. Programs will include cyber security spending in presentation of IT budget requests, as an indicator of delivering value, as a factor in root cause analyses, and as a prerequisite to be evaluated prior to acquisition review and approval.
- Open Data – Programs will report quarterly to the DHS CTO Open Data Manager regarding the status of publically available information and web sites supported by cloud computing solutions and services within their IT Portfolio. Programs will include open data statistics in presentation of IT budget requests, as an indicator of delivering value, as a factor in root cause analyses, and as a prerequisite to be evaluated prior to acquisition review and approval.

7. Challenges, Barriers and Mitigations

Previously, agencies such as the DHS have developed systems and applications to operate in protected government facilities with dedicated infrastructure. Although moving to cloud-enabling technologies offers significant benefits, challenges remain. DHS will need to ensure that it does not compromise its missions by trading confidentiality, integrity or availability of data and information in pursuit of the benefits that the cloud services may offer. The table below lists challenges and mitigation activities that will help the DHS achieve the vision described in this document.

Governance and Culture Changes	
Challenge	**Mitigation**
• Managing the adoption of DHS ECS to enable DHS to achieve its IT objectives. • Establishing and maintaining a Cloud First approach. • Lack of governance, consistency between operations, and standard processes between EDCs and solutions causes issues.	• Execute IT Policy that approve/enforce an Enterprise IT services approach throughout the Department. • Establish a comprehensive services governance lifecycle methodology that guides the identification, design, deployment, and continuous operations of IT service solutions. • Publish service design engineering standards. • Develop and publish enterprise computing service reference architectures for IaaS, PaaS, and SaaS. • Produce master service roadmap to better understand what services are being provided and when.
Cybersecurity	
Challenge	**Mitigation**
• Implementing continuous monitoring, handling intrusion detection and alerts, and providing diagnosis and response. • Ensuring that the security posture is not degraded after issuance of FedRAMP and/or DHS provisional authorization. • Maintaining forensic, records management, Freedom of Information Act (FOIA) reporting, and two-factor authentication.	• Provide acquisition regulation, cyber policies, and Continuous Diagnostics and Mitigation (CDM) capabilities to which cloud providers must adhere in order to adequately secure and DHS data and information. • Draft contract, SLA terms, and conditions that are legally enforceable to ensure service providers maintain the protection levels that DHS requires and reporting and escalating incidents in a prescribed manner. • Develop cyber reporting and escalation requirements in a prescribed format.

Network Operations Dependence	
Challenge	**Mitigation**
• Providing access to reliable, remotely delivered services to customers and support personnel. • Ensuring the EDC infrastructure is capable of supporting multi-vendor services.	• Develop an approach to ensure that multi-vendor services do not degrade infrastructure operational services • Establish operational level agreements for each instance of a multi-service provisioned service.
Service Acquisition and Funding Sustainment	
Challenge	**Mitigation**
• Changing from a focus on the acquisition of materiel solutions to the acquisition and consumption of services. • Establishing funding mechanisms that can rapidly adapt to changing demand to sustain the growth of widely used services. • Reducing or eliminating investment in underutilized and underperforming services.	• Establish policies and procedures for budgeting, funding, acquisition, and cost recovery that leverage a "fee-for-service" model. • Use a cloud broker function to manage the use, performance, and synchronized delivery of cloud service offerings. • Develop a budget strategy to fund initial cloud investments across the Department. • Establish standard contract language to address standards, security, privacy, e-discovery, FOIA access, and Federal recordkeeping. • Reduce or eliminate investment in underutilized and underperforming services through SLM periodic reporting.
Data Migration, Management, and Interoperability	
Challenge	**Mitigation**
• Ensuring data ownership and transportability of data from one service provider to another • Ensuring that data and applications hosted in the various service environments can be discovered, accessed, stored, used, and protected among various DHS components and homeland security partners • Ensuring that the hosting of DHS Component data by an external service provider is subject to technical and contractual conditions that facilitate migration of the data to another provider or back to the DHS data owner • Ensuring data interoperability and secure information sharing with homeland security partners.	• Enforce use of risk assessments that consider exposure to the legal, law enforcement, and national security requirements of within the hosted environment. • Ensure Service Level Agreements (SLAs) are written to address DHS information assurance and data confidentiality and availability requirements. • Require and enforce the adoption DHS information sharing approved services to enable enterprise search, discovery, and access of data.

8. Schedule

DHS expects to provide the schedule for achieving the DHS ECS Strategic Plan in 90 days. DHS is currently working with Components to update plans for legacy data center transition/closure, validate current and projected performance and cost metrics for legacy data centers, and provide DHS CIO review of Component's options for achieving optimization goals in legacy data center operations or expediting transition to the ECS environment in the enterprise data centers.

The table below depicts a template that is currently under review as a tool to be used by the Components to capture and report optimization metrics for each data center in inventory.

The savings algorithm is still under construction but will be a calculation applied equally to each data center comparing the average and total cost of each performance metric to the OMB optimization target in the existing legacy environment (to represent the best legacy solution possible) and the enterprise data center ECS environment (to represent the enterprise solution).

Measure	Definition	Calculation	Target	Current (2016)	Data	Plan/Progress				
						FY2016	FY2017	FY2018	FY2019	FY2020
Energy Metering	(%) Percent of total gross floor area (GFA) in an agency's tiered data center inventory located in tiered data centers that have power metering.	Total GFA of Energy Metered Data Centers/ Total GFA of All Tired Data Centers (Agency-owned)	100%	-	Metered					
Power Usage Effectivness (PUE)	(Ratio) Proportion of total data center energy used by IT equipment.	Total Energy Used/ Total IT Equipment Energy Used (Agency-Owned)	≤ 1.5 (≤ 1.4 for new data centers)	-	Total Energy					
					IT Equipment Energy					
Virtualization	(Ratio) Ratio of operating systems (OS) to physical servers.	(Total Server Count + Total Virtual OS)/ Total Physical Servers (Agency-Owned)	≥ 4	-	Total Server					
					Total Virtual OS					
					Total Physical Servers					
Server Utilization & Automated Monitoring	(%) Percent of time busy (measured as 1 – percent of time spent idle), measured directly by continuous, automated monitoring software, discounted by the fraction of data centers fully equipped with automated monitoring.	Average Server Utilization *Percant of Data Center Fully Equipped with Automated Monitoring (Agency-owned)	≥ 65%	-	Avg.Server Utilization					
					% of Data Center Equipped with Automated Monitoring					
Facility Utilization	(%) Portion of total gross floor area in tiered data centers that is actively utilized for racks that contain IT equipment.	Total Rack Count *30 sq.ft/ Total Gross Floor Area (Agency-owned)	≥ 80%	-	Total Rack Count					
					Total Gross Floor Area					
Closures	Closure/Consolidation of legacy centers	TIERED	25%	-	Closures (TIERED)					
		Non-TIERED	60%	-	Closures (Non-TIERED)					
Cost Savings/Avoidance	Agencies shall, by the end of fiscal year 2018, reduce Government-wide annual costs attributable to physical data centers by at least 25%, relative to the fiscal year 2016 IT Infrastructure Spending data submitted to the Federal IT Dashboard.			-						

9. Conclusion

To achieve the DHS ECS goals, all barriers to adoption and transition must be addressed without major delay. The DHS CIO, or delegations, will be the final decision authority and will provide oversight for execution of DHS ECS, exercising appropriate governance to ensure an efficient orchestration of change, and highly adaptive capabilities that must remain within the physical and operational control of the Department. Simultaneously, the DHS and its component's will continue rationalization of existing systems, applications and data sources while determining the most appropriate cloud service / deployment models for migration. DHS intends to rapidly capitalize on FedRAMP and DHS-approved government and commercial cloud providers to the maximum extent possible to reduce sustainment and operating costs, shorten implementation timelines, more

effectively keep pace with emerging technologies, and allow the DHS to take advantage of the larger economies of scale that typically lower costs.

This strategy is intended to drive the Department toward changes required to dramatically improve the delivery and operation of IT, via DHS ECS, that provides tangible benefits to the DHS community. The Department's approach to deliver this strategy will require strong governance authority and continued commitment to greater transparency through regular and open reporting. To achieve the DHS ECS goals, all barriers to consolidation and transition must be addressed without major delay. Governance must ensure mechanisms are in place to coordinate enterprise activities across the Department.