Federal Data Center Consolidation Initiative

2011 Data Center Consolidation Plan & Progress Report

(October 2011)

Version 1.3

Table of Contents

1 Introduction

In March 2003, Congress passed the Homeland Security Act of 2002 (P.L. 107-296), creating a single Department to ensure c and secure borders, welcome lawful immigrants and visitors, promote the free flow of commerce, prevent and deter terrorist attacks, and protect against and respond to threats to the United States. The resulting Department of Homeland Security (DHS) is the Cabinet Level agency formed from the consolidation of 22 agencies, now called components, which existed previously as independent agencies or departments.

Key to the success of the DHS mission is integrating the incumbent workforce, processes, and systems into a unified organization. Consistent with this need, the DHS Secretary stated the objective to centrally manage services, including Information Technology (IT). The DHS Chief Information Officer (CIO) formulated a vision to achieve this objective for all components. The "One Infrastructure" vision requires a common IT infrastructure across all DHS. The product of this endeavor improves information sharing via an enterprise-wide consolidated IT infrastructure, supporting all of DHS's strategic goals and business objectives: awareness, prevention, protection, response, recovery, services and organizational excellence.

The DHS IT infrastructure had been decentralized and redundant. The IT infrastructures of most DHS components are still primarily aligned with the missions of their legacy agencies as opposed to the five missions of DHS as outlined in the Quadrennial Homeland Security Review. The components transmit information via point-to-point connections that tie individual systems and networks in their entirety to other components' systems and networks. Investment strategies, service-level agreements, and performance measures across components are inconsistent and are often IT-centric as opposed to business- or mission-centric, and there is often insufficient interoperability among components.

Data center consolidation is compulsory to the successful execution of the DHS mission. An early objective of the DHS Office of the Chief Information Officer (OCIO) Information Technology Services Office (ITSO) was the creation of the Enterprise Services Division (ESD) and the Data Center Services (DCS) Project. The objective of the DCS project is to coordinate and oversee the provision of services and facilities for the collocation/consolidation of numerous disparate computing facilities that currently support the DHS components. The project's strategic vision is to reduce the number of existing data centers to two secure, geographically diverse locations to minimize infrastructure while enhancing the disaster recovery posture of the Department. While the Department acknowledges this effort as a fiduciary responsibility, it is not without beneficial byproducts.

DHS's consolidation efforts were already underway before the Federal CIO Council launched the Federal Data Center Consolidation Initiative (FDCCI) on February 26, 2010, including the Federal CIO's calling upon DHS CIO Richard A. Spires, and Treasury Department CIO Michael Duffy to lead the initiative. By the end of the 2010 calendar year, the FDDCI was followed by the *25 Point Implementation Plan to Reform Federal Information Technology Management* issued by the White House on December 9, 2010, which included specifications to consolidate at least 800 data centers by 2015. These Federal CIO objectives and the White House's deficit reduction initiatives are now central to reforming IT in the federal government.

DHS continues to refine and follow up with components on this data call to more fully complete and enhance the accuracy of the information contained in the report. A Data Center Consolidation Division (DCCD) government manager is tasked as the FDCCI POC and works with components on a weekly basis to continually refine their data to the fullest possible degree.

2 Agency Goals for Data Center Consolidation

The wake of the 9/11 terrorist attacks exposed limitations in homeland protection, communication, cooperation and data sharing. DHS components supported multiple disparate data centers. The seven wide area network (WAN) entities were complex and had little ability to scale or adapt to change.

In an effort to standardize IT resources, reduce costs, and improve efficiency, DHS has created an initiative to collocate and consolidate the numerous computing facilities currently supporting each of the DHS components. Though a tenet to DHS's purpose, the collective computing environments made data sharing and collaboration challenging. The motivation for a singular homeland security entity is the same driving force behind the DHS consolidation project – consolidate like assets to foster more productive collaboration, facilitate efficient efforts and offer ease of data sharing to aid in the protection of the nation's resident assets.

Such a consolidation effort greatly reduces the redundancy of systems and hardware across computing facilities, resulting in reduced maintenance, management, and administrative costs, and offering a smaller IT footprint to truly implement green IT. Part of the consolidation strategy is the definition and deployment of a Common Operating Environment (COE) whereby a component's equipment is migrated and transformed into common, standardized platforms for server, network, and storage. Embracing a COE and realizing a reduction in the overall computing asset footprint have resulted in reduced system maintenance, management, and administration costs, while a merging of existing operations and maintenance contracts will further reduce overhead and administrative costs.

Additionally, the consolidation efforts will help to standardize IT resource acquisitions across components, as well as streamline maintenance and support contracts that will allow for less complex vendor support to expedite response times in the event of an emergency. It is important to note, however, that, while a consolidation of facilities will ultimately result in a significant cost savings over time, this will not happen overnight. This effort is considered a long-term strategy.

While risk mitigation efforts and network security objectives will maintain a vigilant eye on continual network security, the final result of the consolidation will be an overall reduction in the network security borders.

Initial planning targeted 17 legacy data center sites to be consolidated into the two DHS Enterprise Data Centers (EDCs). These two EDCs are known as Data Center 1 (DC1) and Data Center 2 (DC2).

The number of legacy sites grew over time to a list of 43 primary DHS locations, with many smaller instances that can be considered minor centers or more appropriately server rooms/closets. These 43 primary sites are a composite representation of the total number of DHS data centers. Currently all principal data center assets are targeted to be consolidated from legacy centers to one of the two DHS EDCs by the end of FY15.

Due in large part to a migration-specific Congressional funding appropriation and DHS's focused attention, there was a surge of migration activities in FY10. This trend supports an early identified risk of the consolidation effort. An initial investment is required from the components in order to complete the system migrations. The return on investment is not immediately realized at the component level, and this financial enticement was required before critical momentum was achieved.

The 2005 Program Cost Analysis was conducted to aid in project guidance throughout the project life cycle. The results demonstrated consistency with 2009 and 2011 Return on Investment (ROI) analyses, and aligned with results from progress made thus far. These reports have concluded that, once migration is complete, DHS should anticipate significant overall cost savings to exceed hundreds of millions of dollars per fiscal year.

The project has not been without obstacles. Funding models are based on ability to capture increasing service fees from components, which has resulted in latency in ROI goals. Overcoming conflicting budgetary, scheduling, and operational objectives will remain a challenge until DHS as a whole matures to a singular cohesive agency. The FY 2010 congressional funding allowed for relief of some concerns; however, the Congressional budget delays created delays in funding and implementing FY11 migration projects. Even with these difficulties, DHS is focused on maintaining momentum for the next fiscal year and beyond.

3 Implementing Shared Services/Multi-tenancy

Primary cost savings are achieved by providing common services, utilities, and facilities to multiple customers who had previously enacted these operations independently. Through Shared Services and Multi-tenancy objectives, the expenses and resources identified as overhead are all but eliminated after the establishment of the initial deployment.

The DHS strategic plan was developed with these efficiencies in mind. The plan called for two redundant data centers operated by separate service providers. This relationship allows for both competitiveness of cost of services and coordination of service portfolios so the data centers provide for maximum efficiencies, scalability and redundancy. In an effort to consolidate similar technology needs, the Department desires to have common operating environments established in each of the data centers to institute efficiency and effectiveness in its operations.

The DHS OCIO ITSO is the executive sponsor of this program and will define future enhancements to the base capability in a service roadmap coordinated with the component representatives. OCIO's Enterprise System Development Office (ESDO), an organization also under the DHS CIO, is the department's executive sponsor of this program. The ESDO development and test environment will be leveraged to support the functions for the COE environments. These environments, also under the managed-service control of the data center vendors, are designed to mirror the production environment.

These "As-a-Service" offerings from DHS OCIO computing are a further investment in the cloud computing approach being planned by DHS. Internal private, external public, and hybrid cloud models are under evaluation to determine how they may best facilitate data center consolidation and DHS mission objectives. Email as a Service (EaaS) has already been implemented and Components are actively migrating to it. Additional applications are currently being evaluated to determine if their services make good candidates to deploy in this new architectural approach.

Following EaaS, additional offerings are planned in order to move the DHS Enterprise Data Centers toward a cloud environment. The following chart summarizes the planned offerings.

Private /Public	IaaS SaaS PaaS	As-a- Service	Abbrev.	SOO Finalized	SOO Issued to Vendors	Contract Awarded /CLINS Available Today	Production and ATO
Private	SaaS	Email	EaaS				
Private	IaaS	Authentication	AUTHaaS				
Public	IaaS	Enterprise Content Delivery	ECDaaS				
Public	PaaS	Identity Proofing	IDPaaS				
Private	PaaS SaaS	SharePoint	SPTaaS				QTR 4 FY11
Private	SaaS	Project Server	PSaaS				QTR 4 FY11
Private	SaaS PaaS IaaS	Dev-Test	DTaaS			QTR 4 FY11	QTR 1 FY12
Private	IaaS	Production	PRDaaS			QTR 4 FY11	QTR 1 FY12
Public	PaaS	Web Content Management	WCMaaS			QTR 4 FY11	QTR 1 FY12
Private	PaaS SaaS	CRM	CRMaaS			QTR 4 FY11	QTR 1 FY12
Private	IaaS	Workplace	WPLaaS			QTR 4 FY11	QTR 2 FY12
Private	SaaS PaaS	Business Intelligence	BIaaS	Planned FY12	Planned FY12	Planned FY12	Planned FY12

DHS remains committed to continual evaluation of cloud services and other technologies as they emerge and mature to invite practical application.

4 Agency Approach, Rationale and Timeline

DHS has been in the process of consolidation and migration for several years. The general consolidation schedule in Section 6.1 shows completed efforts, as well as ongoing and planned activity for the 43 designated primary DHS data center sites (these include those sites that are designated to be the size specified by the FDCCI process, as well as those that were previously tracked and reported by DHS at the Congressional level).

The current approach to migrating components' computing systems and infrastructures to the DHS EDCs involves five general phases with distinct sets of activities, as well as specific deliverables (as outlined in the graphic below). Experience has demanded the process remain under the constant watch of program directors who invoke a cycle of continual improvement. This has resulted in a living and continually improving plan. While the core foundation of the plan has not deviated from inception, several mid- and low-level details have evolved.

Five Phased Approach
Phase 1: Initiation

The Initiation Phase is triggered by the component requesting service from the DHS Data Center Consolidation Division (DCCD) to migrate a legacy system, or to set up a new system capability at an EDC. The component receives an engagement package, and an informational kickoff meeting is held with the DHS data center team to review the package documents including the Data Requirements Questionnaire and Equipment List.

The component submits the required documentation, including a Statement of Work (SOW), IGCE, BOM/ROM, and related attachments such as rack elevations for review and clarification. When all required documents are submitted, a Procurement Request (PR) Package is developed and submitted to ITAC (Information Technology Acquisition Center).

Phase 2: Discovery/Assessment
The Discovery/Assessment Phase is the time to review and solidify all of the engineering, funding, and security requirements for the project. A Request for Proposal is developed and delivered to the Managed Service Providers (MSP). Multiple reviews and discussions, including a technical evaluation of the project proposal, are conducted until the MSP signs and submits project proposal.

Once the component agrees to the proposal, the DHS Contracting Officer's Technical Representative (COTR) signs the proposal and returns it to ITAC. ITAC then writes a contract between the vendor, component, and DHS Headquarters for the specific data center migration work. Finally, the ITAC contracting officer ratifies the contract, and upon signature, planning begins for the data center's migration.

During this Phase the component also undertakes systems/application mapping, relating relationships between software, hardware, and middleware. DCCD and the MSP engineering group works with the component to develop the necessary documentation to migrate the hardware and/or application including rack elevations, floor plans, power requirements, patching documentation, etc. as needed for the specific data center selected for migration to the EDC.

During Phase 2, the component reviews the security requirements, change management process, and begins document preparations for the change requests and Certification and Accreditation (C&A) process that will be necessary in the execution phase. This phase results in completed project documents, an interagency agreement (IAA), a master device list, a ROM, and a funded task order.

Phase 3: Planning Migration
At this point, a kickoff meeting is held at the component's location. The task order and finalized Statement of Work (SOW) are reviewed, and a project plan and schedule are developed.

The MSP Customer Advocate works together with the component to plan process integration, establish approval criteria, and develop a high-level engineering design document. A concept of operations (CONOPS), the migration plan, schedule baseline, and technical and cost baselines are finalized.

Phase 4: Execution
In the Execution phase, the funded contract is implemented by the MSP. The EDC customer advocate serves as the single point of contact into the service support and delivery infrastructure.

The DHS COTR monitors the progress of the migration project through completion, and the Customer Relationship Manager (CRM) works with the component throughout the process.

Facility work, such as rack stand up and power connections, is normally required for any new installation. When facility work is required at the Data Center 1 (DC1) EDC, the NASA Facility Manager is involved.

The Execution Phase begins the change management process, including required Change Requests (CR) and C&A explained earlier in this document. Before production begins, the component will work with the Chief Information Security Officer (CISO) to process CRs and receive the Authority to Connect (ATC), and then the Authority to Operate (ATO).

Upon completion of the migration plan and the initiation of the new processes to provide service in accordance with the SOW, all equipment, applications, and data is turned over to the data center operations team, operations and maintenance (O&M) begins, and the project moves into the Closeout Phase.

Phase 5: Closeout
During project closeout, a post-migration review is conducted, lessons learned are identified, procurement audits are performed, and issues discovered throughout the project are resolved and documented. When the migration process is complete and verified, the systems transfer to O&M.

As a final stage of migration, the components are responsible for undertaking and documenting the decommissioning of their legacy data center space and equipment.

5 Agency Governance Framework for Data Center Consolidation

The objective of the DHS governance framework is to measure and manage project performance and risk. These are crucial elements to the success of such a massive and complex undertaking. DHS diffuses risks through the controls applied by governance boards, procurement and services acquisition approvals, and change management procedures.

For example, at DHS Headquarters, the Information Technology Services Governance Board (ITSGB) and the Infrastructure Change Control Board (ICCB) perform oversight of the EDC migration program activities.

The ITSGB, which is chaired by the Deputy CIO and is composed of component Deputy CIOs, ITSO's executive director, and appointed advisors, is responsible for:

- Proactively evaluating all facets of IT services utility makeup and operations to constantly ensure effective policies and practices are in place, and to identify, validate, and implement improvements that will strengthen the venture and/or its contributions to its customers.
- Expending equivalent diligence in overseeing the integrity, compliance, and performance of those same elements in delivering reliable, high quality, service, and cost-effective results to utility customers consistent with Service Level Agreements (SLAs).

The ICCB, which is composed of a cohesive team of experts who have a holistic vision of DHS's missions and objectives, is responsible for:

- Assuring compliance with all appropriate federal and departmental policies, directives, mandates, and applicable regulations set forth by DHS oversight bodies.
- Ensuring that DHS IT infrastructure changes are planned, engineered, tested, coordinated, and approved before their release. Quality change impact analyses and successful change implementations maximize the uptime of mission-critical systems, applications, and networks.

The ICCB is essential to ensure a seamless transition to ongoing operations. For IT projects that have a Product Readiness Review (PRR) or an Operational Readiness Review (ORR), and impact the operation of the DHS infrastructure areas under the ICCB charter, a CR must be created in the DHS ICCB Remedy tool. Appropriate gate review documentation, such as a detailed implementation and communication plan, and an email from the Information System Security Official (ISSO) endorsing the change, must be attached, and the ICCB process must be followed.

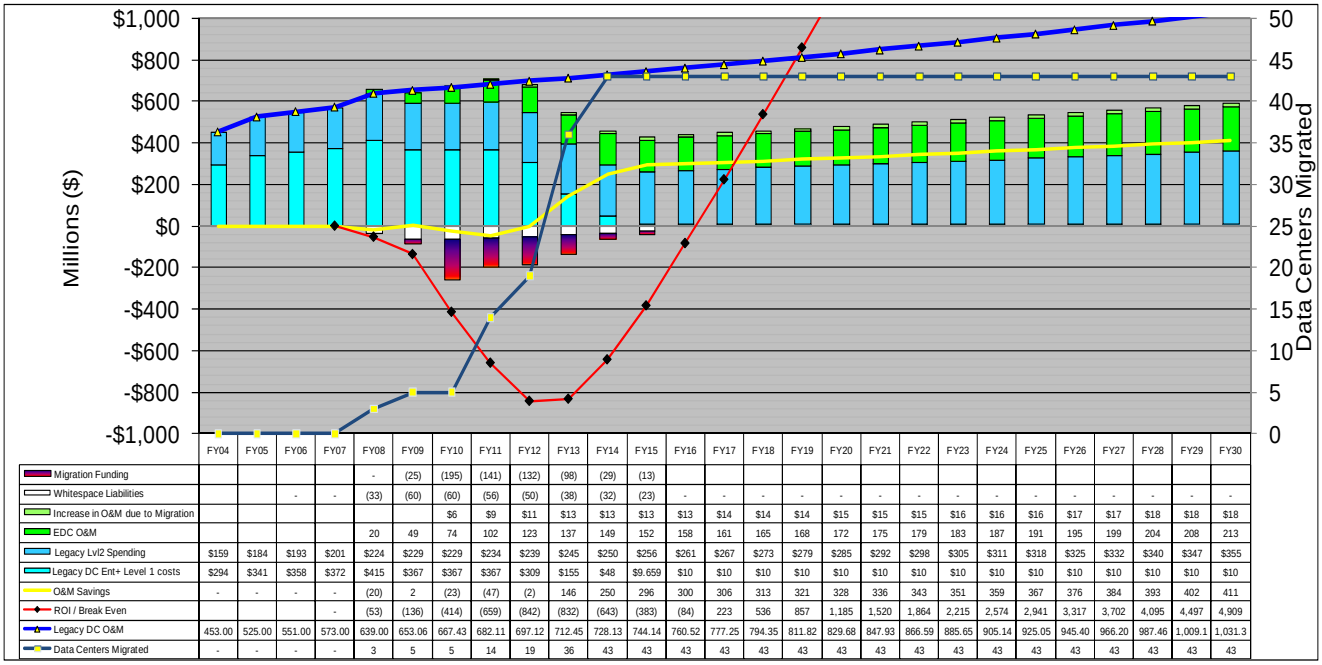
The Systems Engineering Life Cycle (SELC) can be a helpful resource as you plan your migration project. SELC is a guiding framework that provides a vocabulary, order, and description of the activities enabling efficient and effective delivery of capability to users. It provides the common description and process understanding for applying systems engineering in an organization.

After change implementation, a post-implementation vulnerability scan is required for all changes affecting the security posture of a system.

5.1 Cost-Benefit Analysis

Reducing the overall computing asset footprint will result in reduced system maintenance, management, and administration costs, while a merging of existing operations and maintenance contracts will further reduce overhead and administrative costs.

A graphic from an internal DHS Enterprise Data Center ROI analysis conducted in July 2011 is depicted in Exhibit 2.



	FY04	FY05	FY06	FY07	FY08	FY09	FY10	FY11	FY12	FY13	FY14	FY15	FY16	FY17	FY18	FY19	FY20	FY21	FY22	FY23	FY24	FY25	FY26	FY27	FY28	FY29	FY30
Migration Funding					-	(25)	(195)	(141)	(132)	(98)	(29)	(13)															
Whitespace Liabilities			-	-	(33)	(60)	(60)	(56)	(50)	(38)	(32)	(23)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Increase in O&M due to Migration							$6	$9	$11	$13	$13	$13	$13	$14	$14	$14	$15	$15	$15	$16	$16	$16	$17	$17	$18	$18	$18
EDC O&M					20	49	74	102	123	137	149	152	158	161	165	168	172	175	179	183	187	191	195	199	204	208	213
Legacy Lvl2 Spending	$159	$184	$193	$201	$224	$229	$229	$234	$239	$245	$250	$256	$261	$267	$273	$279	$285	$292	$298	$305	$311	$318	$325	$332	$340	$347	$355
Legacy DC Ent+ Level 1 costs	$294	$341	$358	$372	$415	$367	$367	$367	$309	$155	$48	$9.659	$10	$10	$10	$10	$10	$10	$10	$10	$10	$10	$10	$10	$10	$10	$10
O&M Savings	-	-	-	-	(20)	2	(23)	(47)	(2)	146	250	296	300	306	313	321	328	336	343	351	359	367	376	384	393	402	411
ROI / Break Even				-	(53)	(136)	(414)	(659)	(842)	(832)	(643)	(383)	(84)	223	536	857	1,185	1,520	1,864	2,215	2,574	2,941	3,317	3,702	4,095	4,497	4,909
Legacy DC O&M	453.00	525.00	551.00	573.00	639.00	653.06	667.43	682.11	697.12	712.45	728.13	744.14	760.52	777.25	794.35	811.82	829.68	847.93	866.59	885.65	905.14	925.05	945.40	966.20	987.46	1,009.1	1,031.3
Data Centers Migrated	-	-	-	-	3	5	5	14	19	36	43	43	43	43	43	43	43	43	43	43	43	43	43	43	43	43	43

Exhibit 1 - DHS Data Center ROI analysis.

Enterprise Data Center costs shown include all DHS Headquarters and component migration funding. Of note, even though cost savings for additional legacy data centers are not included in the ROI, the trending indicates reduced costs, thereby validating the consolidation strategy.

When migrations to the Enterprise Data Centers are complete, DHS anticipates a $200M reduction in annual costs. With 'Break Even' projected in FY 2017, the cost-benefit to DHS in favor of the consolidation strategy is clear. Cumulative savings/cost avoidance from FY 2017 thru FY 2030 is $4.9B. The migration cash flows shown in this analysis result in an Internal Rate of Return (IRR) of 21%. The IRR is inclusive of relevant migration investments from FY08-FY15.

5.2 Risk Management and Mitigation

The DCS risk management process is based on paradigms developed at the International National Council on Systems Engineering (INCOSE) and the Software Engineering Institute (SEI). This process defines a set of continuous activities to resolve DCCD risk in a systematic and structured way. These paradigms have been tailored to suit DCCD needs. Exhibit 3 describes the DCS structured process elements for managing risks for DCCD. The process represents a set of activities that are executed continuously throughout the life cycle of the project. The steps are both sequential and continuous as new risks emerge.

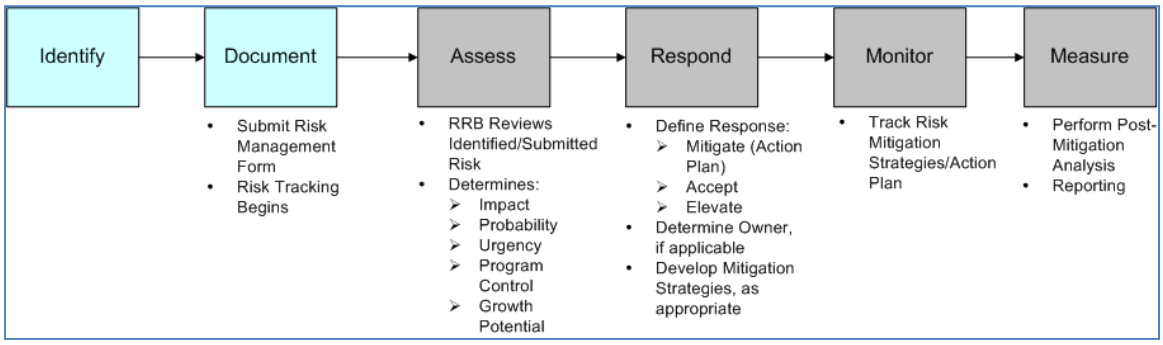


Exhibit 2 – Data Center Risk Management Process.

The communication of risks is the key to a successful risk management process. During weekly status and DCCD meetings, specific risks and mitigation plans may be identified and mutually developed. In addition, the Risk Review Board (RRB) will meet on a monthly basis and may meet at any other time deemed appropriate for emergency actions. This enables the DCS risk management process to be a continuous, evolutionary process where risks and their associated mitigation plans may be reviewed, analyzed, and closed, as necessary

Migration risks are managed using the DCS Project Risk Management Plan. The DCS Project Risk Management Plan describes how risks are identified, documented, evaluated (assessed), prioritized, and monitored on the project, and describes the strategies used to respond to project risk. It describes the control mechanism(s) used to monitor and direct all risk activities. The plan establishes a series of events that, when executed, result in the identification of all risks, the assessment of the impact of risks and the corresponding effect on the success of the project, and the identification of mitigation plans to reduce exposure or loss if these risks are realized. Additionally, it outlines the manner in which risks are handled and/or controlled throughout the development life cycle and includes the regular review and re-assessment of risks to determine the status of mitigation actions. The plan is used by the DCS project manager and coordinated with all affected groups and individuals.

The DCCD Project Team uses a suite of project management software to define migration risks and describe the impact of the risk, including contingency actions, as applicable. Detailed information is provided for each risk regarding the symptoms/triggers for risk realization, as well as the preventative plan(s) and/or contingency plan(s) suggested for risk mitigation.

The DCS Risk Management Plan defines the approach, methodology, and roles and responsibilities for execution of risk management for the DHS Data Center Migration Program. The methodology presented in this plan is intended to accomplish the following:

- Ensure early identification of potential risks
- Promote management of potential risks
- Lessen the impact of a risk that is realized
- Provide project and program visibility to potential risks
- Enable risk metrics and reporting through continuous monitoring
- Enhance the ability to control risks related to operations, performance, schedule, and cost
- Improve communications between the customer and supplier
- Provide a team approach to risk management
- Promote buy-in and commitment
- Ensure metrics-based decision making result

The purpose of risk management is to identify and mitigate potential impacts to the program performance, schedule, and cost. This plan establishes the procedure to be executed by the DCS team to achieve that end. DCCD will work with the DHS components, DCCD, the Enterprise Data Centers, and technical organizations to proactively manage the risks throughout the program and provide regular status updates on risks and their mitigation progress. The Risk Management Plan is an adjunct to the Project Control Plan and System Engineering Integration Master Plan.

5.3 Acquisition Management

The acquisition organization, with technical coordination from the components and the Infrastructure Transformation Program (ITP) Program Management Office (PMO), has a mature and streamlined acquisition process to ensure all such activities are accomplished in the most cost-efficient, schedule-effective manner possible. Coordinating requirements and allowing industry involvement early in the process not only allow DHS to receive better, more informed solutions, but they also allow industry to prepare for requirements in the future. DHS meets regularly with an Industry Advisors panel that provides input during the design and development of project requirements. These efforts do not, however, preclude DHS from pursuing traditional acquisition approaches where situations and requirements may warrant. Furthermore, through the establishment of multiple awards, indefinite delivery/indefinite quantity (IDIQ) contracts for small and large businesses, DHS has developed the capability to meet IT requirements in a streamlined manner through task order competitions.

For each of the projects, the components in conjunction with the ITP Project Management Office (PMO) determine the appropriate source list based primarily on market research and current asset spending. The ITP pursues a balance of large businesses and small business, HUBZone small business, small disadvantaged business, and women-owned small business concerns consistent with DHS socio-economic goals when identifying prospective sources that could meet the individual initiative requirements.

Specifically, the EAGLE IT support services and the First Source Commodities contracts provide significant prime contracting opportunities for small businesses of all categories. These opportunities do not require the small businesses to compete directly with large businesses, thus further ensuring that DHS meets its small business contracting goals.

The DHS Information Technology Acquisition Center (ITAC), an organizational component of the Office of Procurement, serves as the centralized center of excellence for department-wide IT acquisitions. The ITAC provides the ITP access to procurement best practices that follow the path of industry and other federal agencies toward the centralization and consolidation of the department's buying mechanism for IT commodities and services.

The ITAC is responsible as the overarching procurement office within DHS for the contract administration of any enterprise-level contract vehicles or agreements. Individual task orders under these contract vehicles and small buys of less than $5M are managed by the component Procurement Offices to include inspection and acceptance. The ITAC Governance Structure defines the specific details related to contract administration procedures.

The ITP is responsible for ensuring the accurate and timely completion of procurement requests (PRs). All DHS program offices currently initiate, develop, and submit PRs consistent with the ITP Procurement Management Guidance set forth in this document. In this capacity, the ITP requires the following:

- The ITP Director has signature authority to initiate PRs
- PRs must be submitted no less than 120 days in advance of procurement action (see Section 5)

- IT acquisitions of $2,500,000 or more require DHS CIO or Deputy CIO approval to include a MD0007.1 mandatory checklist to be completed by the project manager or component
- All PRs must be on the ITP Spend Plan in the amounts specified in the plan. Any deviations require a revision to the spend plan
- All PRs must track to a milestone in the component project schedule
- All PRs should identify future year O&M requirements, if applicable. components must provide this information with their statements of work (SOWs) and independent government cost estimates (IGCEs)
- Program/project managers and technical leads must provide accurate and complete PRs/SOWs to ensure:

  – Quicker concurrence/approval of PRs by the CIO
  – Reduced Procurement Action Lead Time (PALT) and a timely award
  – More responsive and complete proposals from prospective bidders
  – Awards that are consistent with the pre-award intentions of the parties
  – Fewer changes in contracts, interagency agreements (IAAs), and orders after award
  – Successful delivery/performance/compliance after award
  – Timely payment of invoices and expeditious contract closeouts

5.4 Communications Strategy

A performance-based communications approach is in place to align communications activities in a structured, proven framework to support a project's objective while demonstrating results. Project stakeholders are defined as anyone with an interest or stake in the project, both internal and external to DHS, who are impacted by or will benefit from the data center migration in varying degrees. Thus, it is important to segment stakeholder groups and tailor communications approaches to achieve a desired cognitive level. For some stakeholders e.g., Customs Border and Protection (CBP) and Infrastructure Transformation Program management, this strategy targets communications activities toward achieving a behavior change generating positive perceptions of the program's performance expectations, management objectives and value to DHS strategic goals. For other stakeholders e.g., U.S. Government Accountability Office, Office of Management and Budget, Members of Congress, DHS employees, and end-users, the focus is on how communications activities build and maintain awareness of Enterprise Data Center migrations by providing information about project status, general function, benefits, impacts and progress toward mission completion.

Exhibit 4 illustrates the DCCD communications approach as it has been implemented throughout the life cycle of each migration phase.

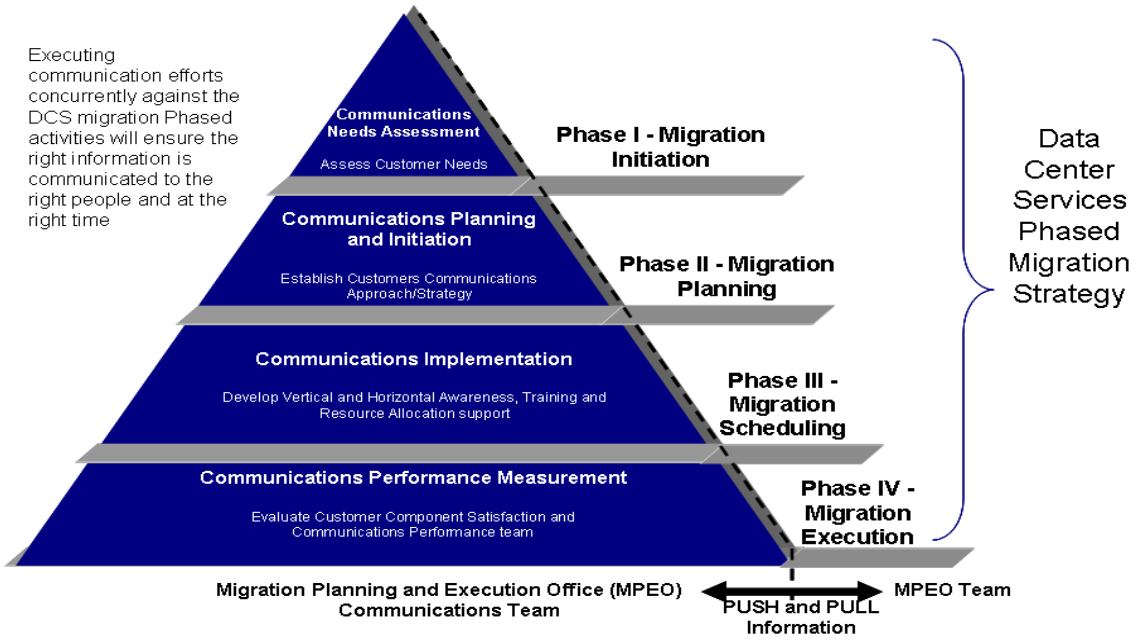


Exhibit 3 - DCS Communication Strategy.

6 Progress

6.1 FDCCI Consolidation Progress

DHS was engaged in consolidation activity for several years before the FDCCI process was initiated. Prior to the FDCCI, five data center locations completed consolidation to the DHS Enterprise Data Centers.

As part of the first year of the FDCCI process, the DHS goal was to complete the consolidation of an additional six of its primary locations by the end of calendar year 2011. Two of these six sites completed migration efforts, while the other four are still planned to complete by the end of calendar year 2011.

For 2012, DHS has allocated FY11 funds to assist component migration efforts, and projects that have been initiated. An additional ten primary sites are planned to complete migration activity by the end of 2012. Principal challenges in implementing consolidation plans include:

- Obtaining planned Congressional funding – beginning in FY 2010, DHS allocated specific migration funds to assist component consolidations. Congressional cuts and delays in providing the funds have prevented timely execution of consolidation activity.
- Consolidation is a multi-stakeholder operation and requires immense amounts of coordination. Delays and issues arise when various stakeholders maintain differing visions, expectations and commitment to the effort.
- DHS is initiating several efforts to cultivate more expeditious consolidation in particular the implementation of "As-a-Service" offerings (detailed previously), and components transitioning to a host of these offerings will expedite migration and reduce the cost of consolidation.
- Streamlined procurement – DHS created a team to facilitate projects through the procurement process.

The planned consolidation completion timeline of primary legacy DHS sites is shown in the High-level Migration Schedule below.

DHS LEGACY DATA CENTER MIGRATION COMPLETION TIMELINE	before 2010	2010	2011	2012	2013	2014	TBD
Customs and Border Protection (CBP)	1		1			1	
Immigration and Customs Enforcement (ICE)				2			
National Protection and Programs Directorate (NPPD)				4			
U.S. Citizenship and Immigration Services (USCIS)					6	1	
DOJ- based data centers (ICE, USCIS, US-VISIT)			2				
Federal Emergency Management Agency (FEMA)			2	2	4	2	
Transportation Security Administration (TSA)	1		1	1	1	2	
U.S. Coast Guard (USCG)					2		1
U.S. Secret Service (USSS)				1	1		
DHS Headquarters (DHS HQ)	3				1		
Total	5	0	6	10	15	6	1
	Total All	43					

Note: While major migration activity is planned to complete by the end of 2014, minor consolidation activity may continue through 2015.

EDC Migration Success Stories

DHS HQ's Data Centers consolidated in 2008

- In FY 2008, two of DHS HQ's primary legacy data centers were part of a single contract and jointly moved to Data Center 1 (DC1). The cost of operations was reduced by approximately 21%. Functionality was improved in information systems and physical security. The total OY1 EDC O&M cost was $15.2M which covers substantially more applications than what was moved from the legacy data centers.

CBP's Commercial Recovery Facility (CRF) consolidated in 2008

- CBP's Commercial Recovery Facility (CRF) data center facility completed migration to DC1 in FY 2008. The cost of operations was reduced by approximately 38%. The cost of operations after migration is $10.5M/year. Functionality was dramatically improved to include more equipment and services, more network bandwidth and more uptime for users. Before migration, CBP was constrained to facility and equipment use only during declared disasters and semiannual testing. CBP now has unlimited access to equipment and systems. Furthermore, CBP has been able to increase the degree of continuity coverage.

Homeland Secure Data Network Data Center consolidated in 2008/2009

- The Homeland Secure Data Network (HSDN) moved primary systems from its legacy commercial location to DC1 in FY 2008. The backup systems moved to Data Center 2 (DC2) in FY 2009. Functionality improved by establishing geographically diverse operations with data replication, continuity of service and robust and redundant connectivity to national Wide Area Network (WAN) classified infrastructure. The completion of this major milestone further enhances DHS command and control capability and mission success by ensuring continuity of HSDN services. DHS now has enterprise–level secure data capabilities at both EDCs, significantly mitigating the risk of catastrophic system impact.

TSA's primary data center consolidated in 2009

- TSA moved their primary system from its legacy site to DC2 in FY 2009. Cost of operations before migration was approximately $89.2M/year. The cost of operations after migration is approximately 9% lower per year. The move resulted in decreased OneNet costs and in an improved information assurance posture by utilizing centrally monitored WAN / Internet connections into the DHS network zones.

FEMA's commercial-hosted systems consolidated in 2011

- FEMA completed their migration of systems from their commercial hosted facility in FY 2011, including DARTS and DRCR (Disaster Assistance Request Tracking System, Debris Removal Contractor Registry). Because only a small amount of equipment was involved,

cost savings are difficult to ascertain. But it allows FEMA to end the contract, and gain consolidation/co-location benefits with other FEMA systems.

CBP's Automated Commercial Environment (ACE) contracted facility consolidated in 2011

- CBP completed its migration activity from their ACE legacy location to DC2 in FY 2011. This allows CBP to end its facility contract of approximately 2200 square feet, and consolidate with other ACE systems at DC2.

6.2 Cost Savings

As DHS continues to support its two EDCs and must fund the non-occupied areas of the data centers while consolidation continues, there is no overall cost savings as yet (see ROI information in Section 5.1). However, individual project savings have been documented. Additionally, the increased implementation of virtualization and "As-a-Service" offerings will reduce the overall costs of migration and post-migration operations.

Some individual project cost reductions are shown below:

TSA facility consolidated in 2009	Pre-consolidation operational costs: $89.2M/year Post-consolidation operational costs: $81M/year
DHS facilities consolidated in 2008	Pre-consolidation operational costs: $19.2M/year Post-consolidation operational costs: $15.2M/year
CBP Commercial Recovery Facility consolidated in 2008	Pre-consolidation operational costs: $17M/year Post-consolidation operational costs: $10.5M/year

Currently, there are no unanticipated consolidation costs; however, the consolidation effort is particularly susceptible to Congressional funding allocations and delays. In FY 2011, the unanticipated length of Continuing Resolutions was a main factor in the delay of the initiation of planned FY 2011 funded migration projects, impacting the overall schedule of consolidation efforts.