Information Technology Acquisition Advisory Council

DHS FINANCIAL MANAGEMENT SYSTEMS MODERNIZATION EFFORT

A Case Study in Strategic, Operational & Business Failure- 20 Years & Counting

Report to Congress:

House Committee on Homeland Security; House Committee on Oversight & Accountability; Senate Homeland Security & Government Affairs Committee; Department of Homeland Security

April 2023

DHS FINANCIAL MANAGEMENT SYSTEMS MODERNIZATION EFFORT

A Case Study in Strategic, Operational & Business Failure- 20 Years & Counting

Table of Contents

Information Technology Acquisition Advisory Council

EXECUTIVE SUMMARY

Since shortly after the Department of Homeland Security was established in 2003 with the consolidation of 22 disparate components under one Cabinet Secretary and leadership team, the Department has sought to gain insight across the enterprise regarding financial management systems, asset management systems, and procurement management systems by pursuing various efforts under the banner of Financial Management Systems Modernization.

For almost 20 years, the Department has continued to repeat documented failure patterns, refused to leverage commercial best practices and data-driven analysis to inform the process, systematically targeted small business incumbent providers as legacy providers that must be replaced, attempted to direct the outcome of significant procurements, and failed to recognize and acknowledge…or simply chose to ignore…that successful businesses continue to invest in innovation and "modernization" in order to meet the mission requirements of their customers.

The leadership of IT-AAC believes that after almost 20 years of failure and abandoned efforts resulting in billions of documented wasted taxpayer dollars, that Congress must intervene definitively to suspend any and all current activity and allocation of public resources until an independent review and investigation is completed and a new strategy and implementation plan is developed that actually aligns to the needs and mission requirements of the Department and its components.

The most recent failure at the Coast Guard that resulted in the need to maintain a manual process for an extended period of time during a transition process and *cost the taxpayers a billion dollars of unbudgeted funds while also putting mission delivery at risk* is the proverbial straw that broke the camel's back that demands attention and action. IT-AAC would like to understand where did that additional billion dollars come from, what were those dollars spent to do, who authorized applying it to cover for another failed effort, how will those dollars be accounted for, and what will be the accountability rendered? Will a person or persons actually receive consequences, including potential termination, as a result of this significant breakdown and increased risk…particularly to mission delivery?

A new GAO Report just released on February 28, 2023 (DHS Financial Management: Actions Needed to Improve Systems Modernization and Address Coast Guard Audit Issues | U.S. GAO) took a deeper look at the USCG failure. On the cover page of the Report it states:

"Although DHS identified, documented, and tracked metrics to assess Coast Guard's system deployment, DHS found that the system was not achieving expected capabilities. ***This is because DHS did not address and remediate known issues identified in operational testing****. DHS's subsequent operational testing and evaluation of the system found that it was not effective, responsive, or reliable. Therefore, DHS could not proceed to full operational capability of the system. It is now in the process of developing a remediation plan to address outstanding issues.*

DHS risks not fully achieving its goal of deploying systems that produce reliable data for management decision-making and financial reporting if it does not remediate serious issues identified by testing. Resolving deficiencies identified by testing before proceeding to the next phase in the acquisition process can help reduce the risk that future system modernization efforts at FEMA and ICE will not meet mission needs or expected capabilities.

GAO also found that corrective action plans Coast Guard developed to address its fiscal year 2021 audit findings did not always contain all of the data attributes recommended in applicable guidance. For example, although DHS guidance emphasizes the importance of root cause analyses in resolving deficiencies, such analyses were often not done. Therefore, Coast Guard is at an increased risk that its corrective actions will not effectively address identified deficiencies"

IT-AAC fully understands the complexity of the challenge of attempting to consolidate various activities when creating a new entity combining 22 different components. However, IT-AAC also fully understands that such an undertaking is not unprecedented and while each circumstance may have unique characteristics, basic approaches that leverage proven best practices include data driven analysis that identifies opportunities for integration of capabilities; aligning software and services requirements and capabilities; and understanding ongoing investment and innovation. DHS should abandon its approach that drives "rip and replace" based on a theory that existing providers, especially small business, cannot be considered "modern" simply because they have been successfully meeting mission requirements for an extended period of time. These are all essential elements of achieving success.

Selection of providers should be brand agnostic and not an intentional effort to displace capable small business without justification. Modernization should be about good business decisions that are informed by relevant data analysis and adopting innovative solutions while leveraging existing investments, underlying technology, scalability, ROI, validated controls, comprehensive security, and more.

IT-AAC desires to see the Department of Homeland Security achieve success in their efforts to create an enterprise view of their various financial, asset, and procurement management systems. Such a result will undoubtedly produce greater efficiency, productivity, and cost savings. However, the track record as of today is replete with failure after failure, abandoning of efforts before completion, and millions of dollars of wasted taxpayer provided resources. This is unacceptable and largely avoidable.

Even today, the Department is challenged with significant impediments resulting from a procurement approach that intentionally separated a software purchase from a services and integration purchase at a total project cost of at least $4 billion dollars.

IT-AAC remains concerned about the lack of a coherent strategy as well as the manner in which the procurements have been conducted. The decision to separate the effort into two distinct acquisition instruments, one for the software and one for the systems integration services was destined to increase risk and does not rely on the experience of commercial best practices or any type of data driven analysis to support such a decision. Those concerns were articulated in an IT-AAC analysis conducted in 2019 referenced previously in this report and attached here.

IT-AAC- DHS FMS AT HIGH RISK

The flawed process has resulted in multiple protests during the EFiMS and EFSI IDIQ awards and although the legal challenges have ultimately been decided in favor of DHS, it clearly illustrates the serious nature of the failure to deliver a coherent strategy or implementation plan.

There now appears to be confusion and a lack of clarity or transparency regarding the latest planned software deployment. It is not clear whether the solution offered in response to the solicitation by the selected provider is the same solution intended to be implemented by the Department. As mentioned, the awardee is a reseller not a product manufacturer. One of the solicitation responses under the EFiMS procurement was from a reseller representing an incumbent solution provider at DHS who has deployed a particular product for financial services management for some period of time. However it appears that the intention for deployment under the subsequent BPA contract award to that reseller on for software appears to be for a completely different product. In fact, that incumbent provider has retired the previous software and it is no longer available for new implementations. Therefore, this issue demands attention and transparency as the selected software solution will likely consume the most significant share of the $3 billion dollar EFiMS IDIQ vehicle funding

Clarity around the selection and award process, particularly as it regards the EFiMS procurement is necessary to insure transparency and trust in the process. Against what

selection criteria were offers evaluated? What product was actually offered, what product was actually selected, and what product is intended to be deployed?

At the very least, it would appear that the product intended to be deployed by the Department is new, is unproven, is untested, has no history of past performance anywhere at DHS or across the federal government, and also appears to have not yet achieved any type of certification for use. All of this is clearly known to decision makers at the Department.

This raises a legitimate and thus far unanswered question as to why the Department appears to have made a decision to "rip and replace" current incumbent providers that are delivering value and mission success with an unproven software solution that may not even be what was included in the response to the procurement solicitation. This is yet another example of flawed judgment and decisions that ultimately lead yet again to failure and increased risk unnecessarily.

In addition, it appears that the Directorate responsible for the planning and implementation of Financial Management Systems modernization efforts has significant personnel vacancies in leadership roles of responsibility and that a majority percentage of the people in the Joint Program Management Office (JPMO) and Business Integration & Operations group (BIO) are contractors with little direct experience with ERP (Enterprise Resource Planning) and financial management systems. This is clearly a troubling gap that may well have contributed to the failures at the Coast Guard that cost the taxpayers an additional unbudgeted $1 billion dollars. An intervention is essential to any opportunity for success.

It is time to stop the repeated failure patterns, reassess and implement proven best practices supported by data-driven analysis and improve the opportunity to get this right once and for all. **IT-AAC therefore calls on Congress to intervene right away and demand an independent investigation and review that would result in the creation of a strategy and implementation plan that is sustainable and will meet the needs and mission requirements of the various components and the Department at large. Such action is bold, but necessary.** The evidence is compelling and well documented by GAO, the OIG, and others. In order to maintain public trust and credibility, it is imperative that oversight of such documented failure and waste of taxpayer provider resources be investigated and those responsible held accountable.

Report to Congress

IT-AAC's Second Assessment of DHS' FMSM is an urgent call to action for Congress on behalf of mission success at the Department of Homeland Security and on behalf of the American taxpayer. Efforts to help DHS address these long standing issues has been futile.

The United States Department of Homeland Security has wasted millions of taxpayer dollars through failed and abandoned efforts to implement a Financial Management Systems Modernization program with at least 5 documented failures since 2003.

An immediate intervention and course correction with appropriate oversight and accountability is essential.

During the preparation and finalization of this comprehensive Report, the United States General Accountability Office (GAO) released yet another report documenting failures at DHS regarding efforts to implement a financial management systems "modernization" effort. Many of the findings, conclusions, and recommendations in this Report are further validated by GAO.

DHS Financial Management: Actions Needed to Improve Systems Modernization and Address Coast Guard Audit Issues | U.S. GAO

Recently the Department spent a reported $1 billion dollars to address unexpected impacts from the latest system transition failure at the United States Coast Guard. Except from Federal News Network article dated April 13, 2022

"The modernization was not without frustration. During the cutover period, USCG had to shut off the legacy system because the authority to operate, the functionality and the cybersecurity were lacking. The period last three months instead of the planned two, during which time Bennet's team performed 20,000 manual transactions and spent about $1 billion to keep worldwide operations going."

Complete article: Federal News Network, April, 2022

It is imperative that Congress…both authorizers and appropriators…intervene immediately! Members of Congress along with OMB, GAO, OIG and others with oversight responsibility must ask the question…where was the $1 billion dollars spent by the USCG allocated from and who authorized the additional expenditure to address the failure to properly execute the transition from one system to another? What is the accountability for this monumental failure? Has anyone at DHS *ever* been held accountable for the loss of hundreds of millions of dollars from

the documented failed and abandoned efforts to pursue a financial management system "modernization" over the past 20 years? After all of this time and failure, is there even clarity around what is currently attempting to be achieved on behalf of meaningful and measurable mission deliverables, especially in view of the evolving mission space and technology solutions to support its success?

As difficult as it may be to believe, the ongoing debacle around a purported Financial Management Systems modernization effort at DHS may be about to get even worse. DHS recently awarded two 20-year IDIQ (indefinite delivery / indefinite quantity) vehicles, EFiMS (Enterprise Financial Management Systems) and EFSI (Enterprise Financial Systems Integrator) respectively, one to buy software licenses ($3 billion ceiling value) and one to obtain systems integration services ($1 billion ceiling value), with a combined ceiling value of $4 billion dollars. *The most recent example of failure at the US Coast Guard is tangible evidence, as documented in the February / 2023 GAO Report, that current efforts are precarious and potentially puts at serious risk another $4 billon dollars of taxpayer provided resources at DHS.*

Further, the Department awarded a contract for software under the EFiMS vehicle to support financial management systems to a reseller of other manufacturers products…meaning that the contract awardee does not design, manufacture, secure, test, or implement any products themselves…instead they represent other companies who make software products. Who then has the responsibility and liability if the product offered through the selected 3rd party contract awardee does not work, has serious flaws, or is subject to an exploit of a vulnerability resulting in a significant adverse impact?

In addition, the Department appears to be planning to deploy a software product that may not be what was offered in the bid submission by the 3rd-party reseller. Clarity is required. Does the solution bid by the reseller require any type of operational or security certification prior to deployment? How was a selection decision made to deploy a brand new software product that is not proven, has no installed footprint across the federal government much less DHS, and may have not even completed any type of process or testing to demonstrate that the solution meets the required technical, operational, and security requirements and actually works as reported.

Further, according to DHS's own documents it appears that the ability to meet various requirements of the software deployment will rely on configuration efforts by the selected systems integrator provider, who may or may not have any experience with the selected software. Once again, given the fact that there is currently no installed footprint established by the chosen software product, the risk of failure is unnecessarily increased by such an approach. How can such a decision process be considered as prudent and productive on behalf of the required mission deliverables, particularly in view of current and past failures?

One method previously used to derive assurance that a Federal financial system COTS (Commercial Off The Shelf) software actually works as intended was a JFMIP certification (Joint Financial Management Improvement Program) or an FSIO certification (Financial Systems Integrity Office). These were rigorous certifications conducted by designated Federal government entities, and were relied upon by other federal agencies. Although JFMIP and FSIO certification processes are no longer available, most Federal financial system COTS solutions in use across the federal government today were subject to these rigorous certification processes in the past.

More recently, the Treasury Department Financial Management Quality Service Management Office (FM QSMO) is establishing a new evaluation process, so that COTS vendors to the federal market can demonstrate functionality of their Federal financial management systems before they are authorized to offer those products / solutions to federal agencies through the FM QSMO Marketplace. *It does not appear that the software solution selected by the Department of Homeland Security has been subject to the rigors of any such performance, functionality, or security evaluation.*

An alternative source of affirmation that a COTS software solution actually works and delivers the functionality it promises would be through the experience of an existing installed base where an agency is using the product and can attest to its functionality through current and past performance. However, in this case, neither option is available to validate the viability of the selected solution.

This means that the Department is once again embarking on a high risk and highly questionable FMS "modernization" initiative that does not include the benefit of any data driven analysis. It also appears that the bulk of the $4 billion "modernization" funding will be spent on a handful of components within the Department versus what was originally intended to be an enterprise solution investment across the entire Department. What is the current strategic, operational, and security plan for the Department as it regards financial management, asset management, and procurement management systems?

A comprehensive risk assessment must be mandatory that includes an examination of current and ongoing impact of repeated failures to mission objectives, deliverables, and outcomes. This assessment should also focus on determining root cause(s) of the previous unsuccessful attempts at modernizing DHS's financial management systems. Lessons learned and recommendations for avoiding future failures should be required of this risk assessment.

As the Department has still not completed any data-driven analysis to support the current decision making process, with no apparent consideration of commercial best practices to help inform such a challenging implementation, with a series of repeated failure patterns over the

past almost twenty years as documented by GAO, OIG and others, it is essential that Congress intervene immediately. All authorized, appropriated, allocated, and approved funding should be suspended immediately and a thorough investigation conducted to review these matters, including how $1 billion dollars can be spent to cover the most recent example of those that failed to properly, securely, and successfully implement the transition effort at the United States Coast Guard. The evidence of a lack of competence and oversight is compelling and must be addressed.

BACKGROUND

The Information Technology Acquisition Advisory Council (IT-AAC) is a non-profit, public-private partnership that was organized in 2007 at the urging of Members of Congress and leadership of the United States Department of Defense. IT-AAC is a trusted "Do Tank" that does not manufacture or sell any product, but rather, operates as an honest broker in the public interest working to improve government – industry collaboration on important matters such as IT modernization; digital transformation; procurement reform and agile acquisition; cloud computing migration and implementation; cybersecurity and critical infrastructure protection; supply chain risk management; DevSecOps; and the application of Artificial Intelligence and Machine Learning; among others to achieve improved efficiency, productivity, and cost-effectiveness, all in support of mission objectives and mission outcomes.

The intent of this Report is to raise awareness in Congress and the Executive Branch and to drive a comprehensive review and immediate corrective action related to the continuing waste of taxpayer dollars being allocated to the ongoing flawed approach being pursued by the Department of Homeland Security to achieve an enterprise view of financial management, asset management, and procurement management across the Department.

For almost two decades the United States Department of Homeland Security has been pursuing an effort to implement a Financial Management Systems Modernization effort to include asset management and procurement management across the enterprise that was newly constituted in 2003. Efforts thus far have been unsuccessful resulting in documented failure after failure and billions of taxpayer provided resources wasted in the process. Congress must intervene immediately in order to triage the hemorrhaging of taxpayer dollars without accountability and force a course correction with actions and milestones that may once and for all achieve the mission results that were anticipated when these various efforts began almost 20 years ago.

The Department of Homeland Security has failed to conduct a data-driven analysis of current capabilities and investments across the various components; has failed to clearly articulate what exactly they are trying to achieve with current efforts and how it impacts mission deliverables; has failed to leverage commercial best practices to inform steps and processes that will support a coherent, concise, and sustainable set of objectives; has failed to complete, maintain and then maximize utilization of an inventory of existing software licenses purchased for implementation or integration of capabilities; has failed to fully implement requirements for full and open competition in federal procurement, and has consistently repeated documented failure patterns over almost 20 years, leading to continuing failure, project abandonment, and wasted taxpayer provided dollars.

Even now, the most recent iteration of the DHS effort is stalled by yet more challenges. There appear to have been additional protests filed but may have ended up being withdrawn. The Enterprise Financial Management Systems (EFiMS) procurement for software and the Enterprise Financial Systems Integrator (EFSI) procurement for associated services were issued separately and are estimated to cost approximately $4 billion dollars even though the current scope and scale of the initiative appear to have been pared back from the original Department-wide plan which included all components, and now appears to be specifically targeting a subset of those components which just happen to be currently utilizing existing small business COTS providers. Contract awards have been made for each procurement, however challenges remain to a successful deployment.

IT-AAC prepared an analysis of the challenges around this ill-advised acquisition strategy in November, 2019 and even then recommended an intervention by Congress to avoid continued failure and waste of taxpayer dollars. IT-AAC- DHS FMS AT HIGH RISK

As further evidence of the alarming nature of the continuing failures and lack of any meaningful accountability, particularly with DHS leadership responsible for the stewardship of taxpayer investment for these purposes, the recently published Report issued by the Office of the Inspector General issued on November 15, 2022 illustrates ongoing deficiencies in oversight, leadership, and accountability for Financial Management across the Department.

https://www.oig.dhs.gov/sites/default/files/assets/2022-11/OIG-23-02-Nov22.pdf

While the independent auditor's Report provides an unmodified (clean) opinion on DHS' consolidated financial statements, the auditor issued an adverse opinion on DHS' internal control over financial reporting as of September 30, 2022. The auditor's report identified material weaknesses in internal control in four areas and other significant deficiencies in two areas. The auditor also reported instances of noncompliance with two laws and regulations. The details of this recent report as well as ongoing GAO reports undisputedly supports the need for Congress to demand the immediate creation of a Plan of Action & Milestones for remediating the ongoing deficiencies in management, oversight, accountability, acquisition process, results measurement, and cost effectiveness of any further investment in efforts to advance a Financial Management Systems Modernization program, and that regular reports are provided to Congress articulating and validating progress against the implementation of the POAM.

On Page 1.3 of the OIG Report, it states *"DHS continued to have deficiencies in its design and implementation of controls related to information technology. These deficiencies have persisted since the inception of DHS."*

In addition, in recent weeks Govini Research has published a new research paper STATUS OF DEPARTMENT OF HOMELAND SECURITY FINANCIAL MODERNIZATION COST which provides an in-depth analysis of expenditures, failures, and more over the past 20 years. A key insight from the analysis says…

"Most importantly, Govini found no evidence of a DHS assessment to determine the total cost of transitioning Federal financial management systems. Such analysis would be a prerequisite for informed decision making of system transitions."

Accordingly, the Information Technology Acquisition Advisory Council (IT-AAC) recommends that Congress take the necessary steps to suspend all funding currently appropriated for this effort and engage an independent review of these matters to inform and recommend a course of action that includes a comprehensive risk assessment and a concept of operations for achieving an integrated enterprise financial management system necessary to provide substantive and timely data required to make informed and prudent decisions that also includes asset management and procurement management across the Department.

Twenty years and at least five documented failed efforts later, wasting millions and even billions of taxpayer provided resources, the Department continues to repeat failure patterns of the past and has yet to demonstrate competence in advancing a strategy and implementation plan in an efficient, effective, productive, prudent, and measurable manner.

First Attempt: eMerge2

Failed $52 million project

Date: 2003-2006

The project was **Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency**, known by the acronym **eMerge2**. DHS started gathering requirements for eMerge2 in December 2003, less than a year after the new Department was formed. Per the eMerge2 RFP: "When DHS was established, twenty-two agencies with disparate management functions were merged. As a result, the Department inherited numerous redundant management functions, business processes and information technology. A tremendous amount of effort is underway to move the Department towards the goal of "one DHS.""

1. The eMerge2 goal was to buy one single system for Department-wide use. Per the eMerge2 RFP: "The eMerge2 solution will provide the capabilities specified in the eMerge2 functional and technical requirements for the following business areas:

· Accounting and Reporting;

· Cost and Revenue Performance Management;

· Asset Management;

· Acquisition and Grants Management; and

· Budget

In addition to providing the capabilities for the domains listed above, the eMerge2 solution must be able to integrate with the future Human Resources Management System (HRMS), one of the e-Travel systems mandated by the General Services Administration (GSA) and the e-Payroll system from the USDA National Finance Center (NFC)."

At the time eMerge2 was conceived, the idea that one enterprise business system could address all business needs was the norm. The requirements for eMerge2 reflected this monolithic ERP concept.

2. DHS awarded a blanket purchase agreement, potentially worth up to $229 million, to BearingPoint in fall 2004 for the Electronically Managing Enterprise Resources for Government Efficiency and Effectiveness (eMerge2) initiative.

3. GAO reports indicate DHS spent $52 million on eMerge2, including $18 million in contractor costs, before the project was deemed a failure, and cancelled in 2006.

4. No specific causes for the project failure were given by DHS management.

Reference:

GAO: DHS lacks strategy to consolidate financial systems - FCW

DHS scuttles Emerge2 program - GCN

Second Attempt: TASC Round One

With Brand Name Justification (Oracle & SAP), Cancelled due to Protest

Date: June 2007-February 2008

1. In June 2007, DHS launched its second attempt to modernize its financial system. This project was called **Transformation and Systems Consolidation (TASC).** This procurement included a brand name justification, indicating DHS had selected the Oracle and SAP financial systems as the baseline for this initiative.

2. In November 2007, DHS sought to procure contractor support for the TASC effort. In January 2008, this solicitation bid was protested, on the basis that the underlying decision to use Oracle and SAP financial systems as the TASC baseline should have been fully competed, to comply with applicable legal and statutory requirements. In February 2008, the courts ruled in favor of the protest, and prohibited DHS from moving further with the procurement as issued.

Reference:

GAO-10-210T Financial Management Systems: DHS Faces Challenges to Successfully Consolidate Its Existing Disparate Systems

Page 2 of this GAO report states in last para: "The initial TASC approach was to migrate its component systems to two financial management systems—Oracle Federal Financials and SAP

Third Attempt: TASC Round Two

With Excessively Restrictive Requirements, Cancelled due to Protest

Date: November 2010-March 2011

1. In January 2010, DHS issued a new RFP for **TASC**. The RFP did not specify any brand names, but stated: "The contractor shall provide an integrated financial management, asset management and acquisition management system solution and perform TASC support services on an IDIQ basis. The financial, acquisition, and asset management enterprise applications will be provided as an integrated solution that is currently fully operational in the public sector."

2. In November 2010, DHS awarded TASC to CACI, a $450 million award over 10 years.

3. In November 2010, two companies protested DHS's award of its TASC program to CACI, on the grounds that the requirements for TASC were overly restrictive and impeded competition.

4. In March 2011, GAO upheld one of the contractor protests and subsequently DHS cancelled its award to CACI.

Reference:

DHS Cancels Solicitation for Financial Management System Amid New Requirements (defensedaily.com)

DHS cancels $450M financial system modernization, considers cloud instead - Washington Technology

DHS cancels $450M award to CACI | Federal News Network

DHS ditches unified financial management system - Nextgov

Fourth Attempt: TRIO

Implementation Project by using a Federal Shared Service Provider (FSSP), costing over $100 million

Dates: August 2014-2016 (IBC)

Dates: December 2017-2022 (IBM)

1. By August 2014, DHS had entered into an agreement with the Interior Business Center (IBC), a Federal Shared Service Provider, to modernize systems for the Domestic Nuclear Detection Office (DNDO), Transportation Security Administration (TSA), and the U.S. Coast Guard (USCG) at a cost of $79 million, an initiative know as **TRIO.**

2. Since this was an agreement with another Federal organization, no commercial competition was needed for this shared service contract.

3. Costs for the project ballooned to over $124 million as of August 2017, about 60 percent more than the original estimate, due in part to unnecessary customization of a COTS solution.

4. The plan to migrate DNDO, TSA, and USCG to an IBC solution, under the TRIO project, did not achieve desired outcome due to a number of problems, including insufficient product delivery, incompatible expectations, and unnecessary customization, despite a year-long discovery process.

5. DHS paused the program twice, the first time in 2015 and again in 2016 when the relationship with IBC was terminated. Poor performance management is the culprit.

6. Further, on December 26, 2017, DHS awarded a new $82.6 Million task order contract to IBM to provide TRIO related support services, using an existing BPA vehicle, EAGLEII, which was typically used to secure IT services.

Reference:

Article:

House Approps Committee faults DHS, Interior alike for shared services failure | Federal News Network

Hill Testimony:

- DHS FINANCIAL SYSTEMS: WILL MODERNIZATION EVER BE ACHIEVED? (govinfo.gov)

Testimony states the following:

"By August 2014, DHS had entered into an agreement with the IBC to modernize systems for the Domestic Nuclear Detection Office, Transportation Security Administration, and the U.S. Coast Guard at a cost of $79 million.

Congressional watchdogs at GAO, or the Government Accountability Office, warned in 2013 that DHS had an increased

risk of, among other things, investing in and implementing systems that do not provide the desired capabilities and ineffectively use resources during its financial system modernization efforts.

GAO's prediction came true. Costs for the project have ballooned to over $124 million as of August, about 60 percent more than the original estimate."

Fifth Attempt: TRIO implementation Project

With IBM as the Systems Integrator goes live in Jan 2022 – then costs over unanticipated $1 billion in manual processing due to legacy migration and customization problems, and puts USCG's mission activities at risk.

Dates: December 2016-January 2022

The TRIO solution, which uses Oracle EBS as the federal financial system, is the flagship modernization project from DHS – highly publicized as a success, after it finally went live in Jan 2022:

United States Coast Guard Transitions to State-of-the-Art Financial Management System | Homeland Security (dhs.gov)

But since going live, there have been serious problems, some of which have been publicly reported.

Lawmakers flag concerns with payment delays, cost overruns for Coast Guard's new financial system | Federal News Network

DHS OIG Report- November / 2022

Page 1.5 & Page 1.10 provide details specifics about the failure by USCG to adequately identify, analyze or respond to risks associated with various business processes and also provides details regarding the background, conditions, causes, and effects of the various failures.

Per the first article - after USCG went live in Jan 2022, they had to spend approximately $1 billion to keep operations running because of cutover issues with old system. An unplanned $1 billion was spent to conduct tens of thousands of manual accounting transactions in order to maintain operations. Clearly the transition to a "modernized" system was not properly

prepared and tested to create a seamless experience. Where did those $1 billion dollars get allocated from? Were resources intended for mission support diverted and instead used for manually process transactions the previous way rather than through a new system?

Out of the woods with financial system, Coast Guard can turn attention to industry | Federal News Network

From that Federal News Network article from April, 2022 – "*The modernization was not without frustration. During the cutover period, USCG had to shut off the legacy system because the authority to operate, the functionality and the cybersecurity were lacking. The period last three months instead of the planned two, during which time Bennet's team performed 20,000 manual transactions and spent about $1 billion to keep worldwide operations going.*"

4. In addition, please find a link to a list of USCG financial system project problems that were posted on the USCG website in October, 2022. These are additional examples and validation of the transition failure from the previous system.

https://www.dcms.uscg.mil/ppc/news/Tag/212040/financial-systems-modernization-solution/

ALCOAST 377/22 - OCT 2022 FSMS INCIDENT MANAGEMENT TEAM STATUS UPDATE (govdelivery.com)

It is striking to note the affirmation that the transition failure created significant risk to USCG mission operations as articulated in the attached passage. e.g. *"Issues related to data migration, systems interfaces, and overall system functionality resulted in significant impacts in the Coast Guard's ability to procure and contract supplies and services and manage funds, thereby adversely impacting our operations, mission support, and our people. "*

These problems were also reported in HS Today online in Oct 2022:

Coast Guard Slashes Backlog of Old Invoices But Has 'Not Yet Attained Stability' in FSMS Transition - HS Today

On February 28, 2023, GAO released a new Report with scathing findings related to the DHS Financial Management Systems Modernization efforts with a special focus on the recent documented failure at the United States Coast Guard

DHS Financial Management: Actions Needed to Improve Systems Modernization and Address Coast Guard Audit Issues | U.S. GAO

IBM has been the systems integrator for TRIO since 2017, after DHS terminated its contract with Interior Business Center (IBC) at Department of Interior, a Federal Shared Service Provider (FSSP), when that earlier project failed at a cost of over $100 million. More recently, the IBM task order was recompeted and awarded to Deloitte.

Sixth Attempt: New Financial System RFI

Issued in March 2018 and in Dec 2018, final RFP issued in Oct 2019 (EFiMS Solicitation)

Dates: **TBD**

1. In March 2018, DHS issued a new RFI, to obtain knowledge of current and innovative technologies within the market for Federal financial software systems.

2. Per the issued RFI, DHS was seeking Federal Financial, Procurement and Asset Management Systems (FPAMS). In Dec 2018, a second RFI was issued, and the name of this procurement was changed from Financial Procurement and Asset Management Systems (FPAMS) to Enterprise Financial Management System (EFiMS). DHS decided to pursue an acquisition strategy that completely separated the software procurement from the services procurement. They determined to issue two separate parallel BPA solicitations – one for SI services (EFSI) worth $1 billion, and one for software (EFiMS) worth $3 billion.

3. The final EFiMS solicitation was issued on Oct 30, 2019. For EFiMS, at least one pre-bid protest and two other protests were filed by two different offerors...

4. DHS eventually awarded EFiMS IDIQ vehicle to Mythics, Carahsoft, and CGI Federal.

5. One of the offerors on the software solicitation (EFiMS) also bid on EFSI solicitation for systems integration services, and was one of 7 contractors (and the only small business) awarded that BPA contract in Nov 2020.

6. In December 2022, DHS awarded two task orders under EFiMS vehicle to Carahsoft, a reseller for other product manufacturers, for implementation at FEMA and ICE CUBE (ICE, USCIS, S & T, CISA,). Both of those awards were subject to protests which were subsequently withdrawn.

FINDINGS & CONCLUSIONS

1. A primary original purpose of a consolidation and “modernization” of financial management systems across the enterprise was driven by an objective in a newly formed Department of 22 merged components to achieve a “clean” financial audit for

the organization and for the oversight authorities including Congress. That objective has not been relevant for some time as the Department has achieved clean audit opinions since 2013, though internal control issues remain persistent.

2. There is no visible strategic plan that includes a coherent set of goals and objectives for financial management, asset management, and procurement management across the Department to provide a on-demand enterprise view of those integrated systems to inform the decision making process.

3. There is no published strategic or operational implementation plan or a Plan of Action and Milestones to achieve an integrated Department-wide enterprise view of financial, asset, and procurement management.

4. There is no apparent plan at the Department to leverage existing software licenses and investments already made, along with technological innovation to achieve an integrated enterprise view of the Department's financial and business operations. Rather, the Department continues to pursue an outdated "rip and replace" modernization approach, with no data-driven analysis to support that path and to the ongoing detriment of forward progress.

5. DHS leadership appears to be committed to a "modernization" approach for financial management and business systems that is focused on eliminating incumbent providers. Many of those same incumbent companies, including small business providers, have been delivering productive and cost-effective solutions producing measurable results while meeting or exceeding mission requirements and deliverables for years. Many of those providers continue to earn customer satisfaction accolades from the components they serve. An approach to "modernization" that ignores performance and innovation, and simply pursues an ill-advised "rip and replace" direction, is likely to create unnecessary disruption and introduce new and potentially serious mission risk as was evidenced with the failed Coast Guard transition.

6. DHS has acknowledged the need to maintain existing engagements with current providers even after the planned transition phase due to the instability of the transition process and the risk to operational capabilities.

7. DHS appears to lack an understanding of industry investment in innovation and ongoing investments to "modernize" capabilities based on customer requirements and evolving technology.

8. DHS has never conducted a data-driven analysis to assess current providers and identify opportunities for integration of existing capabilities that could reduce time, cost, and

risk while improving opportunity for achieving desired objectives.

9. There is no evidence to suggest that DHS has explored or even considered proven commercial best practices utilized to frame successful outcomes for financial management systems integration and “modernization”.

10. DHS has spent hundreds of millions of taxpayer provided resources in failed and abandoned efforts to pursue Financial Management Systems modernization since 2003.

11. DHS has continued to repeat failure patterns that have been documented in GAO and OIG reports with little if any consequential accountability.

12. The original scope and scale of the Financial Management Systems modernization effort was Department-wide and included all 22 components. Today it appears that notwithstanding budget authorization based on a Department-wide initiative, the Department has now reduced the scope and scale to include slightly more than a third of the components across the Department.

13. DHS embarked upon a new acquisition approach to Financial Management Systems modernization by separating into two separate and distinct procurements - one for software and one for integration services. Such an approach is inherently flawed and creates unnecessary risk.

14. The Directorate responsible for the current iteration of the DHS attempt to pursue Financial Management Systems modernization with a combined cost ceiling of $4 billion dollars is primarily staffed by contractors with apparently little experience in ERP. In addition, almost all of the government leadership positions responsible for oversight of the program appear to be vacant.

RECOMMENDATIONS

1. Congress should immediately suspend all activity and spending on DHS financial management systems “modernization” efforts pending further detailed review as indicated in the following.

2. Congress should direct leadership of the Department of Homeland Security in collaboration with the Office of Management and Budget to articulate strategic objectives for a Department-wide capability to achieve a consolidated, enterprise view of financial management, asset management, and procurement management necessary to better support decision making and mission effectiveness.

3. Congress should direct the leadership of the Department of Homeland Security to initiate a data-driven analysis of all existing systems and solutions currently supporting various components across DHS with financial management, asset management, and procurement management capabilities, including customer satisfaction responses from those components, as well as opportunities for solution integration and business automation opportunities. The goal would be to deliver more timely, efficient, productive, and cost-effective results to inform decision making in support of mission objectives and deliverables.

4. Congress should direct the leadership of the Department of Homeland Security to provide an up-to-date inventory of all current licenses purchased and unused for solutions around financial management, asset management, and procurement management capabilities, along with an inventory of any integrated solution opportunities that have not yet been implemented or leveraged.

5. Congress should direct leadership of the Department of Homeland Security in collaboration with the Office of Management and Budget to establish a Plan of Action and Milestones (POA&M) necessary to meet the Strategic Objectives identified in Recommendation #2 to provide clarity as to the forward direction, delineate the immediate, short-term, and long-term priorities; and designate which current components will or will not be included in the Department-wide effort articulated by the strategic objectives.
6. Congress should direct leadership of the Department of Homeland Security in coordination and collaboration with the Office of Management and Budget and the General Services Administration to consider an option of leveraging the FM QSMO Marketplace being established by Treasury Department Financial Management Quality Service Management Office (FM QSMO) to ensure the quality, performance, capability, and security of financial management systems to be utilized across the Department of

Homeland Security.

7. Congress should direct leadership of the Department of Homeland Security to establish an oversight and accountability framework, including an overall risk assessment related to any future effort to advance a “modernization” effort around financial, asset, and procurement management, whether at the enterprise or component level of implementation. This is proven to be an absolute requirement in order to avoid any repeat of the failure at the United States Coast Guard which required $1 billion dollars to mitigate. This is also proven to be a requirement given the alarming number of vacancies in key government leadership positions responsible for financial management systems “modernization”.

8. Congress should direct the leadership of the Department of Homeland Security in collaboration with the Office of Management and Budget and the General Accountability Office to conduct a thorough review and assessment of the recent EFIMS procurement process to understand how a software solution that has no installed base in government and no past performance as was required by the solicitation could be an award winner on the EFiMS IDIQ / BPA vehicle and subsequently be awarded two separate task orders.

9. Congress should establish a reporting cadence of updates to Congress and Committees of jurisdiction on the implementation of each recommendation and elicit assistance from GAO and the OIG to affirm those reporting results in order to maintain external oversight and accountability in an effort to avoid documented and repeated failure patterns of the past on behalf of the mission owners and the American taxpayer.