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

October 2023

This IT-AAC DHS FMSM Readiness Assessment is an urgent call to action for Congress regarding mission success at the Department of Homeland Security (DHS) and on behalf of the American taxpayer. The United States DHS has wasted millions of taxpayer dollars through failed and abandoned efforts to implement a Financial Management Systems Modernization program with at least five documented failures since 2003. An immediate intervention and course correction with appropriate oversight and accountability is essential.

While preparing and finalizing this comprehensive Report, the United States General Accountability Office (GAO) released yet another report documenting failures at DHS in implementing a Financial Management Systems (FMS) "modernization" effort. As a result, the GAO further validates many of the findings, conclusions, and recommendations in this report.[1]

The Department recently spent $1 billion to address unexpected impacts from the latest system transition failure at the United States Coast Guard (USCG).[2] "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 lasted three months instead of the planned two, during which Bennet's team performed 20,000 manual transactions and spent about $1 billion to keep worldwide operations going."[3,4]

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 were the 1 billion dollars spent by the USCG allocated from, and who authorized the additional expenditure to address the failure to execute the transition from one system to another properly? What is the accountability for this monumental failure?

[1] https://www.gao.gov/products/gao-23-105194

[2] Federal News Network article dated April 13, 2022

[3] https://federalnewsnetwork.com/defense-main/2021/10/the-coast-guard-prepares-for-a-new-financial-management-system/

[4] https://federalnewsnetwork.com/it-modernization/2022/04/out-of-the-woods-with-financial-system-coast-guard-can-turn-attention-to-industry/

Has anyone at DHS ever been held accountable for losing 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 given 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 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 USCG is tangible evidence, as documented in the February / 2023 GAO Report, that current efforts are precarious and potentially put at severe risk another 4 billion dollars of taxpayer-provided resources at DHS.

Further, the Department awarded a contract for software under the EFiMS vehicle to support the 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 is responsible and liable 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 differ from what was offered in the bid submitted by the 3rd-party reseller. Clarity is required. Does the solution bid by the reseller require any operational or security certification before 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 process or testing to demonstrate that the solution meets the required technical, operational, and security requirements and works as reported.

Further, according to DHS's 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 designated software. Once again, given that the chosen software product currently establishes no installed footprint, such an approach unnecessarily increases the risk of failure. How can such a decision process be considered prudent and productive on behalf of the required mission deliverables, particularly considering current and past failures?

One method previously used to derive assurance that a Federal financial system commercial off-the-shelf (COTS) software works as intended was a Joint Financial Management

Improvement Program certification[5] (JFMIP) or a Financial Systems Integrity Office (FSIO) certification.[6] 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[7] (FM QSMO) is establishing a new evaluation process so COTS vendors to the federal market can demonstrate the functionality of their Federal Financial Management Systems before they are authorized to offer those products/solutions to federal agencies through the FM QSMO marketplace. Unfortunately, it appears the software solution selected by the DHS has yet to be subject to the rigors of any such performance, functionality, or security evaluation.

An alternative source of affirmation that a COTS software solution 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 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 initially intended to be an enterprise solution investment across the entire Department. What is the Department's current strategic, operational, and security plan regarding financial management, asset management, and procurement management systems?

A comprehensive risk assessment must be mandatory to examine repeated failures' current and ongoing impact on mission objectives, deliverables, and outcomes. This assessment should also focus on determining the root cause(s) of the unsuccessful attempts at modernizing DHS's Financial Management Systems. Lessons learned, and recommendations for avoiding future failures should be required for 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, Congress must 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

[5] https://www.cfo.gov/jfmip/
[6] https://fcw.com/2007/06/fsio-to-improve-financial-software-certification-process/230603/
[7] https://www.fiscal.treasury.gov/fmqsmo/

failed to properly, securely, and successfully implement the transition effort at the USCG. The evidence of a lack of competence and oversight is compelling and must be addressed.

EXECUTIVE SUMMARY

Since shortly after the DHS was established in 2003 with the consolidation of twenty-two 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 twenty 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 chose to ignore…that successful businesses continue to invest in innovation and "modernization" to meet the mission requirements of their customers.

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

The most recent failure at the Coast Guard resulted in the need to maintain a manual process for an extended period 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 that additional billion dollars came from, what those dollars were spent to do, who authorized applying it to cover for another failed effort, how those dollars will be accounted for, and what accountability will be rendered. Will a person or persons receive consequences, including potential termination, due to this significant breakdown and increased risk…particularly to mission delivery?

A new GAO Report released on February 28, 2023,[8] looked deeper 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 system evaluation found that it was not effective, responsive, or reliable. Therefore, DHS could not proceed to the full operational capability of the system. It is now in the process of*

[8] https://www.gao.gov/products/gao-23-105194

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. In addition, 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 attempting to consolidate various activities when creating a new entity combining twenty-two 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 businesses, cannot be considered "modern" simply because they have been successfully meeting mission requirements for an extended period. These are all essential elements of achieving success.

The selection of providers should be brand agnostic and not an intentional effort to displace qualified small businesses without justification. Instead, modernization should be about good business decisions informed by relevant data analysis and adopting innovative solutions while leveraging existing investments, underlying technology, scalability, return on investment, validated controls, comprehensive security, and more.

IT-AAC desires to see the DHS succeed in creating an enterprise view of its various financial, asset, and procurement management systems. This result will undoubtedly produce greater efficiency, productivity, and cost savings. Unfortunately, however, the track record as of today is replete with failure after failure, abandoning 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 need for a coherent strategy and how the procurements have been conducted. The decision to separate the effort into two different 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 data-driven analysis to support such a decision. Those concerns were articulated in an IT-AAC analysis in 2019, referenced previously in this report and attached.[9]

The flawed process has resulted in multiple protests during the EFiMS and EFSI IDIQ awards. 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 appears to be confusion and a need for more clarity or transparency regarding the latest planned software deployment. It needs to be clarified 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 time. However, the intention for deployment under the subsequent BPA contract award to that reseller for software seems to be for a completely different product. That incumbent provider has retired the previous software and 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 regarding the EFiMS procurement, is necessary to ensure transparency and trust in the process. For example, against what selection criteria were offers evaluated? What product was offered, what product was 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, unproven, untested, has no history of past performance anywhere at DHS or across the federal government, and appears to have not yet achieved any certification for use. All of this is known to decision-makers in the Department.

This raises a legitimate and thus far unanswered question as to why the Department appears to have decided to “rip and replace” incumbent providers delivering value and mission success with an unproven software solution that may not even be what was included in 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 and Business Integration and Operations group are contractors with little direct experience with Enterprise Resource Planning and Financial Management

[9] IT-AAC- DHS FMS AT HIGH RISK

Systems. This is a troubling gap that may have contributed to the failures of 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. Therefore, IT-AAC calls on Congress to intervene immediately and demand an independent investigation and review to create **a sustainable strategy and implementation plan that 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. To maintain public trust and credibility, oversight of such documented failure and waste of taxpayer-provider resources must be investigated, and those responsible held accountable.

BACKGROUND

The Information Technology Acquisition Advisory Council (IT-AAC) is a non-profit, public-private partnership organized in 2007 at the urging of Members of Congress and the United States Department of Defense leadership. IT-AAC is a trusted "Do Tank" that does not manufacture or sell any product but instead operates as an honest broker in the public interest, working to improve government–industry collaboration on essential 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.

This report intends 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 DHS to achieve an enterprise view of financial management, asset management, and procurement management across the Department.

IT-AAC prepared an analysis of the challenges around this ill-advised acquisition strategy in November 2019 and, even then, recommended intervention by Congress to avoid continued failure and waste of taxpayer dollars.[10]

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.[11]

[10] IT-AAC- DHS FMS AT HIGH RISK

[11] 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 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 support the need for Congress to demand the immediate creation of a Plan of Action and Milestones (POAM) for remediating the persistent 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.

Page 1.3 of the OIG Report 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, Govini Research has published a new research paper in recent weeks.[12] The report, Status Of Department Of Homeland Security Financial Modernization Cost, provides an in-depth analysis of expenditures, failures, and more over the past twenty years. A critical insight from the analysis states: "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 in 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.

EVIDENCE

First Attempt: eMerge2 failed the $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

[12] https://govini.com/wp-content/uploads/2023/03/Govini_DHS-FMS-Spend-Analysis.pdf

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. As a result, a tremendous amount of effort is underway to move the Department toward the goal of "one DHS."

1. The eMerge2 goal was to buy one 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)."

2. DHS awarded a blanket purchase agreement, potentially worth up to $229 million, to BearingPoint in the fall of 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 canceled in 2006.

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

Reference:

- GAO: DHS lacks a strategy to consolidate financial systems - FCW[13]
- DHS scuttles eMerge2 program - GCN[14]

Second Attempt: TASC round one, with brand name justification (Oracle & SAP), canceled 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.

[13] https://fcw.com/it-modernization/2007/06/gao-dhs-lacks-strategy-to-consolidate-financial-systems/230561/
[14] https://fcw.com/it-modernization/2007/06/gao-dhs-lacks-strategy-to-consolidate-financial-systems/230561/

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

Reference:

- GAO-10-210T Financial Management Systems: DHS Faces Challenges to Successfully Consolidate Its Existing Disparate Systems.[15] Page 2 of this GAO report states in the 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, canceled 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, fully operational solution in the public sector."

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

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

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

Reference:

- DHS Cancels Solicitation for Financial Management System Amid New Requirements[16]
- DHS cancels $450M financial system modernization, considers cloud instead - Washington Technology[17]
- DHS cancels $450M award to CACI | Federal News Network[18]
- DHS ditches unified financial management system - Nextgov[19]

[15] https://www.gao.gov/assets/gao-10-210t.pdf
[16] https://www.defensedaily.com/dhs-cancels-solicitation-for-financial-management-system-amid-new-requirements-2/homeland-security/
[17] https://washingtontechnology.com/2011/05/dhs-cancels-450m-financial-system-modernization-considers-cloud-instead/350477/
[18] https://federalnewsnetwork.com/technology-main/2011/05/dhs-cancels-450m-award-to-caci/
[19] https://www.nextgov.com/it-modernization/2011/05/dhs-ditches-unified-financial-management-system/49061/

Fourth Attempt: TRIO, failed implementation project by using a Federal Shared Service Provider, costing over $100 million

Dates: August 2014-2016 (IBC)

Dates: December 2017-2022 (IBM)

1. By August 2014, DHS had agreed 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 USCG for $79 million, an initiative is known as TRIO.

2. Since this was an agreement with another federal organization, no commercial competition was conducted for this contract.

3. Costs for the project ballooned to over $124 million as of August 2017, about 60 percent more than the original estimate.

4. The plan to migrate DNDO, TSA, and USCG to an IBC solution under the TRIO project failed due to several problems, including insufficient product delivery, incompatible expectations, and unexpected delays, 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.

6. 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, typically used to secure IT services.

Reference:

- Article: House Approps Committee faults DHS, Interior alike for shared services failure | Federal News Network[20]
- Hill Testimony: DHS Financial Systems - Will Modernization Ever Be Achieved?21 The testimony states the following:
  "By August 2014, DHS had agreed with the IBC to modernize systems for the Domestic Nuclear Detection Office, Transportation Security Administration, and the U.S. Coast Guard for $79 million.
  Congressional watchdogs at GAO 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."

[20] https://federalnewsnetwork.com/reporters-notebook-jason-miller/2017/08/house-approps-committee-faults-dhs-interior-alike-for-shared-services-failure/
[21] https://www.govinfo.gov/content/pkg/CHRG-115hhrg28418/html/CHRG-115hhrg28418.htm

Fifth Attempt: TRIO implementation Project with IBM as the systems integrator went live in Jan 2022 – then costs over unanticipated $1 billion in manual processing due to migration 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. [22]

But there have been severe problems since going live, some of which have been publicly reported. Page 1.5 & Page 1.10 of the references DHS report provides details about the failure by USCG to adequately identify, analyze or respond to risks associated with various business processes and details regarding the background, conditions, causes, and effects of the multiple failures. [23]

After USCG went live in Jan 2022, they had to spend approximately $1 billion to keep operations running because of cutover issues with the old system. An unplanned $1 billion was spent to conduct tens of thousands of manual accounting transactions to maintain operations.[24] The transition to a "modernized" system was not adequately 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 processing transactions the previous way rather than through a new system?

From that Federal News Network article from April 2022 – "The modernization was not without frustration. During the cutover period,[25] USCG had to shut off the legacy system because the authority to operate, the functionality, and the cybersecurity were lacking. As a result, the period lasted three months instead of the planned two, during which Bennet's team performed 20,000 manual transactions and spent about $1 billion to keep worldwide operations going."[26]

4. Also, please find a link to a list of USCG financial system project problems posted on the USCG website in October 2022. These are additional examples and validation of the transition failure from the previous system.[27]

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

[22] https://www.dhs.gov/news/2022/01/07/united-states-coast-guard-transitions-state-art-financial-management-system
[23] https://www.oig.dhs.gov/sites/default/files/assets/2022-11/OIG-23-02-Nov22.pdf
[24] https://federalnewsnetwork.com/agency-oversight/2022/08/lawmakers-flag-concerns-with-payment-delays-cost-overruns-for-coast-guards-new-financial-system/
[25] https://federalnewsnetwork.com/defense-main/2021/10/the-coast-guard-prepares-for-a-new-financial-management-system/
[26] https://federalnewsnetwork.com/it-modernization/2022/04/out-of-the-woods-with-financial-system-coast-guard-can-turn-attention-to-industry/
[27] https://www.dcms.uscg.mil/ppc/news/Tag/212040/financial-systems-modernization-solution/

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.[28]

On February 28, 2023, GAO released a new Report with scathing findings related to the DHS Financial Management Systems Modernization efforts, focusing on the recent documented failure at the United States Coast Guard.[29]

IBM has been the systems integrator for TRIO since 2017 after DHS terminated its contract with Interior Business Center (IBC) at the Department of Interior, a Federal Shared Service Provider, when that earlier project failed at the 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 published in Oct 2019 (EFiMS Solicitation)

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

2. Per the issued RFI, DHS was seeking Federal Financial, Procurement, and Asset Management Systems (FPAMS). In Dec 2018, a second RFI was published, and the name of this procurement was changed from Financial Procurement and Asset Management Systems (FPAMS) to Enterprise Financial Management System (EFiMS). DHS pursued an acquisition strategy that completely separated software procurement from services procurement. They determined to issue two similar 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 the 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.

[28] https://www.hstoday.us/featured/coast-guard-slashes-backlog-of-old-invoices-but-has-not-yet-attained-stability-in-fsms-transition/
[29] https://www.gao.gov/products/gao-23-105194

Addendum 10-3-2023

DHS Financial Management System Modernization Tech Shortcomings

For over 19 years, DHS has been on a path to update and consolidate its financial systems. DHS has made three attempts during that time but failed to modernize its systems. In 2017, DHS began its fourth attempt, the Financial Systems Modernization (FSM) TRIO program, to address DHS's incompatible financial processes and antiquated systems currently in use department wide. The goal of FSM was to improve the quality of financial information to support decision-making and improve the ability to provide timely and accurate reporting to ensure efficient stewardship of taxpayer dollars. Lessons learned from each sequential and successful go-live were carried through to the next component. DHS deployed the TRIO in order of size and complexity to reduce risk. The first component was DNDO (now CWMD), then TSA, then finally the USCG. In a report produced by the DHS Office of Inspector General in 2020, it was stated that the approach and use of lessons learned from the successful go-lives of the new system that: "DHS's actions provides a positive outlook on the future progress of the FSM TRIO project we make no recommendations for improvement". **Note, DHS received a clean audit opinion the first year the TRIO was live on the modern Oracle system**.

The follow up effort to modernize additional components (FEMA and ICE) went forward under the title of "Enterprise Financial Management System" (EFiMS). During that procurement cycle, vendors were told to propose solutions that had significant track records of success within the Federal Government. In 2022, DHS decided to change direction and selected SAP to expand financials modernization. This decision carries risk on multiple fronts. First, SAP's legacy on-premise product versions are set for end-of-life and retired. End-of-life dates are in both 2025 and 2027. It appears CaraSoft/SAP is planning to provide their legacy financial product to FEMA and ICE, not a cloud version. The cloud solution and combination is completely untested in a complex multi-organizational environment such as DHS. In addition, SAP has already publically announced that there will be no new innovation or enhancement to the product for any on-prem customers.

The footprint shared with the SI community on the EFSI contract is below.

On-Premise:

- *SAP S/AHANA Enterprise Management for Professional use*
- *SAP S/AHANA, Developer access*
- *SAP Access Control for SAP S/4HANA*

- *SAP Enable Now*
- *SAP Extended Procurement*
- *SAP Extended Procurement, Public Sector and Regulated Industries extension*
- *SAP S/4HANA Finance for receivables management*
- *SAP S/AHANA contract, lease and real estate management SAP S/4HANA for asset retirement obligation Management*
- *SAP Tax, Benefits, and Payment Processing for Public Sector for S/4HANA*
- *Ul data protection masking for SAP S/4HANA SAP Enterprise Master Data Governance for SAP S/4HANA SAP BW/HANA*
- *SAP Data Services, enterprise edition*
- *SAP Process Orchestration*
- *SAP Business Planning and Consolidation, version for SAP BWI4HANA SAP BusinessObjects Enterprise*
- *SAP HANA, runtime edition for applications & SAP BW*
- *CFO Control - Small (Includes Data Model, Data Loaders, Reports and Analytics) SaaS:*
- *SAP Analytics Cloud for bi, predictive edition. This is an optional tool that DHS may use in the future.*

Software Hosting

- *Based on the current requirements, DHS has access to on-premise licenses that can be deployed in the DHS Enterprise Cloud.*

This path forward contains an implementation of the SAP on premise application and then a required move to SAP Cloud Apps due to the end of life status, therefore, DHS will in fact be signing up for two disruptive and expensive implementations. This is fraud and waste.

Also, as the existing Oracle financial systems continue to stabilize and be optimized after going live in 2021, (USCG), 2019 (TSA) and 2018 (CWMD), the GAO produced a report to DHS making various recommendations that lessons learned stemming from the Oracle implementation at the TRIO be used for both FEMA and ICE. Those recommendations included process changes around testing and issue remediation before system go-live. Choosing a different vendor and moving away from the product vendor that produced the only progress/success that DHS has had in 20 years is counterproductive to GAO's direction and recommendations.

FINDINGS & CONCLUSIONS

1. An original primary purpose of the consolidation and "modernization" of Financial Management Systems across the enterprise was driven by an objective in a newly formed Department of twenty-two merged components to achieve a "clean" financial audit for the organization and 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 an on-demand enterprise view of those integrated systems to inform decision-making.
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. The Department has no clear plan to leverage existing software licenses, investments already made, and technological innovation to achieve an integrated enterprise view of the Department's financial and business operations. Instead, 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 focused on eliminating incumbent providers. Many 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. In addition, many providers continue to earn customer satisfaction accolades from the components they serve. An approach to "modernization" that ignores performance and innovation and pursues an ill-advised "rip and replace" direction is likely to create unnecessary disruption and introduce new and potentially severe mission risk, as was evidenced by 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 to integrate existing capabilities that could reduce time, cost, and risk while improving opportunities for achieving desired objectives.

9. No evidence suggests that DHS has explored or even considered proven commercial best practices utilized to frame successful outcomes for the Financial Management System 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 documented in GAO and OIG reports with little 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 fit slightly more than a third of its components.
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. However, 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 government leadership positions responsible for program oversight must be occupied.

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 DHS 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 support decision making and mission effectiveness better.
3. Congress should direct the leadership of the DHS 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 supporting mission objectives and deliverables.

4. Congress should direct the leadership of the DHS 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 a list of any integrated solution opportunities that have not yet been implemented or leveraged.
5. Congress should direct leadership of the DHS in collaboration with the Office of Management and Budget to establish a Plan of Action and Milestones 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 DHS 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 the Treasury Department Financial Management Quality Service Management Office[30] to ensure the quality, performance, capability, and security of the Financial Management Systems to be utilized across the DHS.
7. Congress should direct leadership of the DHS 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 to avoid any repeat of the failure at the United States Coast Guard, which required 1 billion dollars to mitigate. This is also 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 DHS 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 to maintain external oversight and accountability to avoid documented and repeated failure patterns of the past on behalf of the mission owners and the American taxpayer.

[30] https://www.fiscal.treasury.gov/fmqsmo/