

IT Capital Planning: Enterprise Architecture and Exhibit 300 processes for the CDC and NNSA

Christopher Furton

Syracuse University

Abstract

This paper explores two of the topics relating to IT Capital Planning and compares those processes in place at two federal agencies. The Enterprise Architecture and the Exhibit 300 business cases are reviewed from the Centers for Disease Control and Prevention (CDC) and the National Nuclear Security Administration (NNSA). The findings are that both agencies have programs in place to address Enterprise Architecture and the Exhibit 300, however, the amount of information made public varies resulting in inadequately level grounds for comparing and contrasting. Regardless, this paper explores the agencies' programs highlighting the positive aspects and the growth opportunities of each while evaluating the overall IT Capital Planning posture.

IT Capital Planning: Enterprise Architecture and Exhibit 300 processes for the CDC and NNSA

This paper will explore two federal agencies in relation to two capital planning topics.

The first agency, the Centers for Disease Control and Prevention (CDC), is an agency within the Department of Health and Human Services (DHHS). The CDC “strives to improve the quality of people’s health in the U.S. and worldwide through an integrated health protection goal approach” (Centers for Disease Control and Prevention, 2008b). The second agency, the National Nuclear Security Administration, is an agency with the Department of Energy (DoE). The NNSA implements programs with major national security endeavors involving nuclear weapons, nuclear nonproliferation, and providing safe and effective nuclear propulsion to the U.S. Navy (U.S. Department of Energy, 2011a).

The CDC and the NNSA are nearly equivalent in financial size with similar budget requests (U.S. Department of Health and Human Services, 2011; U.S. Department of Energy, 2011a). This allows for an appropriate comparison between the agencies on the topics of Enterprise Architecture (EA) and Exhibit 300 submission trends. The format of this paper will begin each topic area with a brief overview of the topic and then provide detailed information about how each agency approaches the concepts. At the end of each topic area, a section comparing and contrasting to the two agencies give insight into the effectiveness and efficiencies discovered. After completion of both topic areas, the conclusion evaluates both agencies overall on both topics and provides recommendations for increased performance.

To adequately analyze each agency’s EA and Exhibit 300 processes, occasional review of higher level policy within the Department of Health and Human Services and the Department of Energy may be necessary. References to the agency’s higher-level organizations will be kept

minimal; however, by nature of both topics, some elements are inherited from senior organizations and are directly applicable and must be considered.

Topic Area 1: Overview of Enterprise Architecture

The Clinger-Cohen Act of 1996 assigned the Chief Information Officers (CIO) of each agency with the requirement to develop information technology architectures. In order to achieve this goal, each agency must develop an architecture that aligns with the cabinet level department's architecture and the top-level Federal Enterprise Architecture. To achieve this, the Federal CIO Council chose a segmented approach that allows departments and agencies to develop architectural segments that integrate into the larger enterprise architecture framework. This method is designed to facilitate the effective and efficient coordination of the lines of business of the Federal Government across the elements of enterprise architecture (The Chief Information Officers Council, 1999).

The Federal Enterprise Architecture (FEA) encompasses the Federal Government's approach to enterprise architecture providing a framework for cross-agency investment analysis, management, and use. This is accomplished by providing five inter-related reference models incorporated into the Consolidated Reference Model (CRM). The reference models are:

- (1) Performance Reference Model (PRM)
- (2) Business Reference Model (BRM)
- (3) Service Component Reference Model (SRM)
- (4) Data Reference Model (DRM)
- (5) Technical Reference Model (TRM).

Using these reference models, agencies can identify gaps, redundancies, and opportunities for collaboration across three general profiles: Geospatial Profile, Records Management Profile, and Security and Privacy Profile (FEA-SPP Working Group, 2010).

To achieve these goals and requirements, each agency develops an EA program to achieve improvements in agency mission performance and other measurement areas. The program helps organize and clarify strategic goals, investments, business solutions, and measurable performance improvements. This forms the results-oriented Performance Improvement Lifecycle comprising of three phases: architect, invest, and implement. This simple value chain links EA with IT investment management and project execution. According to the Office of Management and Budget (2008a), the chief architects and staff support business stakeholders through continuous performance improvement to:

- “identify and prioritize enterprise segments and opportunities to improve mission performance, linked to agency goals and objectives;
- plan a course of action to close performance gaps, using common or shared information assets and information technology assets;
- allocate agency resources supporting program management and project execution;
- measure and assess performance to verify and report results; and
- assess feedback on program performance to enhance architecture, investment, and implementation decisions” (p. 4).

To help agencies with Enterprise Architecture compliance, the Office of Management and Budget developed the EA Assessment Framework version 3.0 (EAAFv3). The EAAFv3 provides a mechanism for agencies to conduct internal diagnostics as well as oversight from the

OMB level. The OMB reviews agency self-assessments and provides detailed feedback on each criterion and an overall final assessment rating. The assessment focuses on the three capability areas: completion of enterprise architecture, use of EA to drive improved decision-making, and results achieved to improve the agency's program effectiveness. Each focus capability area is graded with a color scale where red is bad, yellow is moderate, and green is good (Office of Management and Budget, 2008a).

To aid in analysis of the federal agencies for this paper, a more granular view of Enterprise Architecture is needed. The FEA framework partitions a given architecture into business, data, applications, and technology architectures. The current state of an agency across these four partitions is referred to as the current, or as-is, views. The agencies develop target architectures, or to-be, views based on vision, principles and overall strategic direction. Progress towards the to-be view is governed by standards and transitional processes. These transitional processes contain capital IT investment planning and decision making while the standards contain security, data, application, and technology standards (The Chief Information Officers Council, 1999). Figure 1 in the Figures appendix provides a graphical representation of the Federal Enterprise Architecture Framework.

In summary, the Federal Enterprise Architecture Framework focuses on the business requirements of an agency. It defines the current state of the agency and architects produce the artifacts based off standards and processes ultimately transitioning the agency to the future state. The overall EA framework is developed using segments where each lower leveled bureau, agency, or department owns a slice of the overall architecture. Governance bodies such as the Office of Management and Budget provide oversight by review of agency conducted self-assessments and provides feedback on overall progress based on completion, use, and results

obtained from the EA. The end-state goal of EA to earn value by promoting interoperability, resource sharing, reducing costs, and supporting capital IT investment planning (The Chief Information Officers Council, 1999).

Centers for Disease Control and Prevention – Enterprise Architecture

In order to discuss the Centers for Disease Control and Prevention's Enterprise Architecture program and progress, a brief discussion about the Department of Health and Human Services program is needed. Because EA forms a hierarchical structure, the DHHS framework maps directly to the Federal Enterprise Architecture. This is accomplished through an eight layered model as depicted in figure 2 (Centers for Disease Control and Prevention, 2007):

- 1) Strategy layer – described from the HHS Strategic Plan
- 2) Stakeholder layer – identifies partners and recipients of HHS products and services
- 3) Business layer – business operations of HHS that support the mission
- 4) Data layer – information that HHS needs to perform the business operations
- 5) Systems & Services layer – automated systems and services that create or manipulate data or information
- 6) Technology layer – hardware, software, networks, and standards that comprising technology infrastructure
- 7) Workforce later – job categories associated with performing critical HHS work
- 8) Facilities layer – geographical distribution and locations where work is performed.

The eight layer HHS model encompasses the five reference models of the FEA. Specifically, the Performance Reference Model's uniquely tailored performance indicators map directly to the HHS Strategy layer. The FEA Business Reference Model's lines of business map to the HHS

Business layer. The Service Component Reference Model's service domains and types map to the HHS Systems & Services layer. The Data Reference Model's business-focused data standardization maps to the HHS Data layer. Lastly, the Technical Reference Model's component interfaces map to the HHS Technology layer (Centers for Disease Control and Prevention, 2007). This mapping of the performance and business-driven FEA reference models to the HHS architecture ensures that the HHS and subordinate agencies are compliant with overall EA objectives. See figure 2 for a visual representation.

At the CDC level of HHS, the Unified Process (UP) is the overarching framework and methodology that contains the tools to help project managers follow best practices. The CDC Unified Process contains process guides for enterprise architecture as well as other essential elements such as capital planning, performance measurement, and strategic planning. The Unified Process also contains Practice Guides that provide guidance to teams about key project management practices as well as templates and checklists to facilitate consistency and reduce re-work. The Unified Process can be applied across the agency to address informatics projects as well as general construction and campaign projects to increase efficiency and effectiveness of project management processes (Centers for Disease Control and Prevention, 2012c).

The process guide for EA outlines the process for CDC when developing or updating information systems. Specifically, the process guide initiates an Enterprise Architecture Review process in the Initiating Phase of all projects which helps ensure that project sponsors work with the EA activity team prior to approving a project. This critical process helps sponsors and project managers ensure that the purpose of their projects properly align with the enterprise architecture and the overall CDC strategic plan. The process guide also draws the correlations between enterprise architecture and other information technology processes, discusses timing of

EA during the overall project lifecycle, and associated costs in time and dollars (Centers for Disease Control and Prevention, 2012c).

To support execution of the EA Process Guide and compliance with HHS architecture and FEA architecture, the CDDC developed the Enterprise Architecture Development Method (ADM). This method outlines six-steps: initiation, baseline analysis, target analysis, transition planning, transformation, and compliance. These steps involve early activities within the initiation step progressing towards creation of a current view, transitioning to a future view, and ending at compliance and continuous monitoring (Decker & Fitzpatrick, 2007).

As part of the overall system lifecycle, the CDC has adapted the OMB prescribed Performance Improvement Lifecycle (PIL) for linking goals to IT results. Using the phases of Architect, Invest, and Implement, the CDC has a solid process in place to validate and provide “assurances that a project or investment is addressing specific capability gaps and providing intended performance improvements” (Centers for Disease Control and Prevention, 2009).

As of October 2008, the CDC is well on track with meeting the requirements set forth for segmented architecture. The CDC has “all ready linked all major, tactical, and supporting investments to an EA defined segment” (Centers for Disease Control and Prevention, 2008a). However, public record of an evaluation of the CDC Unified Process on EA is not available from the Government Accountability Office (GAO) or the HHS Office of the Inspector General (OIG).

One significant contributing factor to the success CDC has achieved can be attributed to the structure and dedication of resources. The CDC has established an Enterprise Architecture Program Management Office (PMO) that oversees and provides guidance to CDC program managers. In addition the EA PMO established the Enterprise Architecture Review Board

(EARB) responsible for verifying that project proposals meet the requirements outlined by the EA. The CDC has established EA architecture teams throughout the organization with contracted expertise in supporting segment architecture. Additionally, the CDC has developed EA working groups (AWG) comprised of members across the CDC components that focus on specific EA related topics. For example, the topic of open source software in system development was addressed by an AWG resulting in specific policy for usage of open source software to reduce cost. Lastly, the CDC had developed Standing AWGs for security and for software management that are continuous working groups addressing these two concerns and the impact of each to the overall enterprise architecture (Centers for Disease Control and Prevention, 2007).

National Nuclear Security Administration – Enterprise Architecture

As with the CDC, in order to properly evaluate the National Nuclear Security Administration's Enterprise Architecture program, some discussion of their higher organization will be needed. The Department of Energy's Information Resource Management (IRM) Strategic Plan identifies EA as the fourth objective of the second strategic goal. Specifically, the IRM, developed in 2009, has an objective of developing and maintaining an EA that "allows the Department's Senior Leaders to make informed decisions when managing Information Technology" (U.S. Department of Energy, 2009).

In April of 2011, the DOE Office of the Chief Information Officer published the DOE Enterprise Architecture Enterprise Transition Plan. This plan describes the DOE's high-priority initiatives for migrating the department to the target (or to-be) architecture. To accomplish this transition, the DOE established the EA Governance Framework containing processes and oversight elements at the Departmental and staff office-levels. The specific entities involved in

overseeing the development of the EA are the IT Council (ITC) and the Architecture Review Board (ARB). The review board is comprised of senior members of each Program and Staff Offices which oversees the EA work groups (U.S. Department of Energy, 2009). The DOE also appoints a Chief Architect and establishes the Enterprise Architecture Working Group to coordinate integration of respective program and staff office architectures into the DOE EA (U.S. Department of Energy, 2008).

The DOE has established Baseline Architectures based off the Strategy layer, Business layer, services layer, data layer, and technology layer. Furthermore, EA baseline segments are identified that align with the FEA reference models. The 16 segments identified by DOE include core mission segments, business service segments, and enterprise service segments. At the center of the EA program is the Business Intelligence Tool and Enterprise Repository. This web-based application provides EA and portfolio management reporting and analytical functions to support stakeholders and governing bodies. It captures EA data such as application inventories, segment data, and dependencies across systems (U.S. Department of Energy, 2009).

At the NNSA level, the CIO implementation plan published in 2012 defines a strategic goal for “enhancing our capabilities” by applying “an enterprise architecture approach to redesign the NNSA unclassified networks into one integrated NSE network” (National Nuclear Security Administration, 2011a). Another strategic goal is the “development of enterprise governance process for IT investments” by “establishing a process to identify clear roles and responsibilities for IT projects and ensure alignment with the NNSA Enterprise Architecture” (National Nuclear Security Administration, 2011a).

The NNSA has limited information publicly available about its current progress with Enterprise Architecture. However, NNSA has contracted with Federated IT who develops and maintains an IT strategy and develops the Enterprise Architecture (Federated IT).

Compare and Contrast of Enterprise Architecture

Based off information made available to the public, the Centers for Disease Control and Prevention have established an effective program for management of capital expenses including Enterprise Architecture. In contrast, the National Nuclear Security Administration program is in its infancy and has a long way to go before being truly effective and efficient. Minimally, both agencies have at least acknowledged the need and value of the EA program in context to IT capital planning.

What did the CDC do right?

The CDC fully understands and has made sufficient steps to integrating EA into their overall capital planning practices. Specifically, the Unified Process is the key to success for the CDC (Centers for Disease Control and Prevention, 2012c). By having a centralized function for integrating EA, Program Management, Budgeting, and Capital Planning and Investment Control, the CDC has proven a level of maturity beyond that of the NNSA. In terms of EA, the CDC and the DHHS have established direct linkages between the FEA without reinventing the wheel (Centers for Disease Control and Prevention, 2007). The CDC's Architecture Development Method further emphasizes the role that CDC plays in the overall DHHS architecture. The ADM focuses on providing a method to development segmented architecture supporting the current view (Centers for Disease Control and Prevention, 2007). This aspect seems to be missing from the NNSA program. Lastly, the DHHS has committed \$57.5 Million towards enterprise

architecture (United States Government, 2012) which is just over three times as much as the NNSA.

CDC growth opportunities

In terms of Enterprise Architecture, the CDC is on the right track. Adequate financial commitment and emphasis has been placed on EA within the IT Strategic Plan (Centers for Disease Control and Prevention, 2008b). With the great progress already made, the agency can now focus on continual process improvement. Additionally, the CDC architecture defines two layers that have not been further defined, the Workforce layer and the Facilities layer (Centers for Disease Control and Prevention, 2007). This unique addition by the DHHS offers an interesting mix of human capital with the IT capital planning which may prove useful to the CDC in the future.

What did the NNSA do right?

According to the IT Federal Dashboard, the DOE has committed \$18.6 Million towards Enterprise Architecture (United States Government, 2012). Although the specific investments for those dollars could not be located within the dashboard, the commitment of financial resources at the department level matches the IT Strategy EA goals declared by both DOE (U.S. Department of Energy, 2009) and the NNSA (National Nuclear Security Administration, 2011a). The CDC and the NNSA overall annual budget is nearly identical with \$11.2 Billion (U.S. Department of Health and Human Services, 2011) and 11.0 Billion (U.S. Department of Energy, 2011c) respectively; however, the amount the NNSA contributed to EA is substantially less than the CDC. Lastly, the DOE has appointed the CIO as having the responsibility for the EA program (U.S. Department of Energy, 2008). Assigning responsibility is essential to accomplishing the task and the DOE is on the right path.

NNSA growth opportunities

The NNSA is planning to take the leap into enterprise architecture with the 2012-2016 strategy. Strategic goal 1-1 objectives includes applying an enterprise architecture approach to the current unclassified systems and goal 3-4 focuses on enterprise governance and establishing roles and responsibilities for IT projects and alignment with the NNSA EA (National Nuclear Security Administration, 2011a). The agency has acknowledged that its “current IT investments within NNSA are loosely controlled at best” (National Nuclear Security Administration, 2011a) and has made development of an EA a goal for the next five years.

The DOE Inspector General conducted an audit of the overall DOE Enterprise Architecture program in 2005 with negative results. The IG noted that “the Department had not fully defined its current or future information technology requirements, essential elements if an architecture is to be an effective tool in managing technology investments” (U.S. Department of Energy, 2005). Furthermore, the NNSA did not provide comments on the draft IG report which does not reflect well upon the agency. (U.S. Department of Energy, 2005).

Lastly, the NNSA received scrutiny from the GAO in February of 2011 in an audit on Nuclear Weapons. Among the findings, the GAO found that the “NNSA lacks complete data on (1) the condition and value of its existing infrastructure, (2) cost estimates and completion dates for planned capital improvement projects, (3) shared use facilities within the enterprise, and (4) critical human capital skills” (U.S. General Accounting Office, 2011). This finding further emphasizes the need for the NNSA to establish and utilize an Enterprise Architecture Program.

Topic Area 2: Overview of Exhibit 300s

The exhibit 300 is an essential part of the overall IT capital planning process. The exhibit 300 “is designed to coordinate OMB’s collection of agency information for its reports to the Congress required” by federal law; “to ensure the business case for investments are made and tied to the mission statements, long-term goals and objectives, and annual performance plans” are developed (Office of Management and Budget, 2008b). The exhibit 300 is a one-stop shop for IT management issues pertaining to IT investments. The exhibit 300 is submitted annually along with an agency’s budget submission. The public-releasable exhibit 300 is required to be posted to the agency website within 2 weeks of the release of the President’s Budget (Office of Management and Budget, 2008b).

In the overall IT Capital Planning and Control Process, the exhibit 300 works together with the agency’s Enterprise Architecture program and the exhibit 53. The exhibit 53, which will not be discussed in this paper, is a tool for reporting the funding of the portfolio. The exhibit 300 is further broken down into two documents, the A and B. Exhibit 300A provides detailed justifications for major IT investments where Exhibit 300B manages the execution of those investments through the life cycle. “By integrating the disciplines of architecture, investment management, and project implementation, these programs provide the foundation for sound IT management practices, end-to-end government of IT capital assets, and the alignment of IT investments with an agency’s strategic goals” (Office of Management and Budget, 2011).

The Exhibit 300A is broken down into four sections:

1. Section A: Overview
2. Section B: Investment Detail
3. Section C: Summary of Funding (Budget Authority for Capital Assets)
4. Section D: Acquisition/Contract Strategy (All Capital Assets)

Section A provides a general overview of the investment with a name and unique investment identifier.

Section B further breaks down the investment requiring a brief summary, description of association to

existing performance gaps, and relation to specific legislation. This section further includes progress towards major milestones and accomplishments as well as anticipated out-year budget requests. Lastly, Section B includes contact information for those associated with that investment. Section C is a table listing financial figures for previous years, current year, and future years. Lastly, Section D outlines contract information associated with the investment including statuses, effective dates, descriptions, and earned value management data (Office of Management and Budget, 2011).

The Exhibit 300B is broken down into six sections:

1. Section A: General Information
2. Section B.1: Projects
3. Section B.2: Activities
4. Section B.3: Project Risk
5. Section C.1: Operational Performance Information
6. Section C.2: Operational Risk

Section A provides a general overview of the investment with a name and unique identifier. Section B focuses on project execution data where B.1 lists project information and Program Manager information. Section B.2 lists all activities occurring during the current fiscal year in terms of key deliverables and earned value achieved. Lastly, Section B.3 includes risk assessments for the investment including probability, impact, and mitigation plans. Section C focuses on operational data where C.1 lists operational performance metrics as either results specific or technology specific. Section C.2 lists all significant operational related risks that are currently open including risk impact and mitigation plans (Office of Management and Budget, 2011).

Centers for Disease Control and Prevention – Exhibit 300s

To better understand the Centers for Disease Control and Prevention's exhibit 300 content, the current year (FY-12) Exhibit 300 and the future year (FY-13) Exhibit 300A&B

documents for two major IT initiatives were reviewed. The first initiative reviewed is the CDC Information Technology Infrastructure with a total FY2012 spending of \$78.5M. The second initiative reviewed is the CDC National Electronic Disease Surveillance System with a total FY 2012 spending of \$12.5M.

The CDC Information Technology Infrastructure initiative was reviewed by comparing the FY11 Exhibit 300 (Centers for Disease Control and Prevention, 2012a) with the 2009-2012 CDC IT Strategic Plan (Centers for Disease Control and Prevention, 2008b). Direct correlations were found between the strategic plan and the exhibit 300 on several topics. First, the CDC defined a strategic goal within the Information Technology Foundation as objective 2: “provide office-based and mobile computing power and data storage capacity to support CDC’s mission and operations” (Centers for Disease Control and Prevention, 2008b). This goal is reflected in the Exhibit 300 by acknowledging the need for a mobile CDC workforce and the accomplishment of implementing CDCMail, a private cloud model mail system (Centers for Disease Control and Prevention, 2012a).

In addition to mobile computing, the CDC exhibit 300 has another correlation to the Strategic Plan within Goal Area 5 – Collaborative Work and Innovation. Objective 1 of this goal is to “accelerate innovation in public health by leveraging information technology and processes that support collaborative work” (Centers for Disease Control and Prevention, 2008b). The Exhibit 300 reflects that goal with the accomplishment of establishing a videoconferencing system connecting eight CDC locations (Centers for Disease Control and Prevention, 2012a).

The FY 2012 Exhibit 300B for the CDC’s Information Technology Infrastructure initiative provided excellent insight on performance with addition of Key Performance Indicators and Performance Metrics. All performance metrics for the initiative were met or exceeded including

cost per user (\$5822/user), number of expanded service offerings (+5), number of users supported per IT staff member (78), and service level agreement timeliness (100%) (Centers for Disease Control and Prevention, 2011a). As with the FY11 Exhibit 300, the FY12 Exhibit300A&B has several correlations to the overall IT Strategy including customer-centric IT services, improving service delivery, and providing scientists with need tools via service offerings (Centers for Disease Control and Prevention, 2008b).

The next CDC initiative evaluated is the National Electronic Disease Surveillance System (NEDSS). The FY11 Exhibit 300 and the FY12 Exhibit 300A&B both emphasize the role that this project has in relation to the overall CDC mission and vision. Furthermore, the NEDSS system directly contributes to the core mission to “enable CDC to effectively share knowledge...and deliver health information and interventions using customer-centered... strategies to protect and promote the health of diverse populations” (Centers for Disease Control and Prevention, 2008b). This system also aligns with the CDC Director’s strategic priority to “strengthen epidemiology and surveillance capability” (Centers for Disease Control and Prevention, 2012b).

Despite the overwhelming positive pictures painted by the all the Exhibit 300s analyzed, the FY12 Exhibit 300 A&B shows potentially poor performance based off earned value management within the NEDSS system. Specifically, the comparison of planned work completed and actual work completed shows several activities that have not accomplished the anticipated amount of work. However, in every instance the actual dollar amount cost was significantly lower than the planned costs (Centers for Disease Control and Prevention, 2011b). This data should raise concern among CDC leadership.

National Nuclear Security Administration –Exhibit 300s

To better understand the National Nuclear Security Administration’s Exhibit 300 content, two current FY12 exhibit 300A&B documents were retrieved from the Federal IT Dashboard (United States Government, 2012) and compared to the agency’s 2012-2016 IT strategic planning documents. The first initiative reviewed was the NNSA’s Enterprise Resource Planning (ERP) system with a total spending for FY2012 of \$8.3 Million. The second initiative reviewed was the Advanced Simulation and Computing program named Sequoia with a total spending for FY2012 of \$101.9 Million.

The Exhibit 300A&B for the ERP initiative described a steady state system that has already met a 1.5 year return on investment. The document directly referenced the Department of Energy strategic goal of building a “fully integrated resource management strategy that supports mission needs” as well as the NNSA goal to “create an efficient, effective, and less risk-averse enterprise through simplified business and management processes” (National Nuclear Security Administration, 2011c). The exhibit 300 defines six gaps that were closed by the ERP initiative including Year 2000 (Y2K) issues, manual workflows, manual business processes and operations, data redundancy and inconsistency, cost reporting shortfalls, and costly technical migrations of legacy systems.

When comparing this initiative to the NNSA 2012-2016 CIO Implementation Plan (National Nuclear Security Administration, 2011a), there was a lack of references within the strategic goals of which this initiative would fulfill. However, the initiative could play a minor role in achieving some of the strategic goals but in an indirect manner. For example, strategic goal 1-5 is to “Improve Business Processes” (National Nuclear Security Administration, 2011a). Because the ERP initiative aims to reduce manual workflows by creating electronic or automated

processes, this initiative could improve the overall business processes and contribute to accomplishing that goal.

The next Exhibit 300A&B reviewed is the NNSA initiative for the Advanced Simulation and Computing (ASC) program Sequoia. This initiative is an “uncertainty quantification and weapon science resource” utilized by several weapons laboratories (National Nuclear Security Administration, 2011b). Because of the nature of this classified system, very little information was provided. However, the Exhibit 300A&B provided general information showing that the project manager is qualified to hold the position, that an analysis of alternatives has been conducted, and that the system is not compatible with cloud computing. Furthermore, the Exhibit 300A&B showed a recent update to the project’s risk register. In terms of project performance, the initiative is currently on schedule and under budget.

The Sequoia initiative’s performance metric attributes table shows that the program is substantially meeting the performance indicators. For example, the “intended use” indicator had a target monthly usage percentage of 20% while the actual results were 74% usage. Additionally, the “percent time available” achieved a difficult 99% uptime when the target goal was 75%. Both of these performance indicators emphasize the success of the program.

In terms of strategic planning and Sequoia’s overall role in the capital planning process, the program has earned a “green” rating depicting a successful program. The initiative fits into the agency’s overall strategic plan by contributing to strategic goal 1-5: improving business processes. The exhibit 300A&B briefly mentions the role in Enterprise Architecture but detailed information had been removed due to classification (National Nuclear Security Administration, 2011b).

Despite the quality of the exhibit 300A&B documents, the NNSA has not identified very many major IT investments. Within the Federal IT Dashboard (United States Government, 2012), the NNSA only has four investments: two simulation investments, one classified network infrastructure investment, and the ERP investment. The FY2012 budget document identifies a \$1 Billion dollar IT capital investment portfolio and nearly \$500 Million in other annual IT expenditures (U.S. Department of Energy, 2011b, p. 30). Initial review shows significant IT capital investments not being reported in the Federal IT Dashboard.

Compare and Contrast of Exhibit 300s

Reviewing both agencies' exhibit 300s and assessing the overall contribution to their IT capital planning process was challenging due to insufficient information. Both agencies removed significant information from the exhibits in the public versions. All exhibit 300s that were reviewed did not have detailed information about how the initiative fits into the Enterprise Architecture or information about future budget year projections. However, with the exception of redacting information, both agencies had substantial content in their business cases and supporting documentation.

One unique aspect worth noting is the variance in quantity and quality of information provided between investment initiatives. Within the CDC, the most expensive capital investment was the IT infrastructure project but the corresponding business case was comparatively less substantive than the other initiatives. Similarly, the NNSA's most expensive initiative was the Sequoia program but the business case for that program was also less thorough than the low cost ERP program. When reviewing the business cases for quality, it is the author's opinion that both agencies are lacking substantial information and provided minimal data as required by law.

Conclusion

In conclusion, the Centers for Disease Control and Prevention and the National Nuclear Security Administration both have programs in place to address IT capital planning. However, the agencies' programs cannot be fairly compared with each other to determine which is better. Due to the nature of the NNSA, very little information has been made publicly available about their enterprise architecture program. In contrast, the CDC has made their entire investment control program known as the Unified Process (UP) available to the public. There is ample information available showing that both agencies are addressing enterprise architecture despite the lack of detailed public information.

The review of exhibit 300 documents from both agencies also revealed a similar trend. Both agencies prepare the exhibits as required by law but the details of those documents are removed before being uploaded to the public dashboard repository. This prevents thorough analysis. However, both agencies reference the overall capital planning process including Capital Planning and Investment Control (CPIC) and Enterprise Architecture.

This paper provided insight to the overall capital planning process employed by two federal government agencies. A brief overview of Enterprise Architecture and the Business Case was presented along with a description of how that agency addressed the requirements. When possible, comparisons between agencies provided insight into best practices and identified some shortcomings in processes. While each agency approached the two elements of capital planning in different ways, it was found that both agencies successfully achieved the end-state goal of matching strategic goals to IT capital investments.

References

Centers for Disease Control and Prevention. (2007, June 22). *Enterprise Architecture at CDC*.

Retrieved March 10, 2012, from Centers for Disease Control and Prevention Homepage:

<http://www2a.cdc.gov/cdcup/library/presentations/ea/default.asp>

Centers for Disease Control and Prevention. (2008a, October). *EA Segment Architecture*.

Retrieved March 12, 2012, from Project Management Newsletter:

http://www2a.cdc.gov/cdcup/library/newsletter/CDC_UP_Newsletter_v2_i10.pdf

Centers for Disease Control and Prevention. (2008b). *Information Technology Strategic Plan FY 2009-2012*. Washington, DC: Office of the Chief Information Officer.

Centers for Disease Control and Prevention. (2009, January). *Enterprise Architecture Alignment with EPLC*. Retrieved March 12, 2012, from Project Management Newsletter:

http://www2.cdc.gov/cdcup/library/newsletter/CDC_UP_Newsletter_v3_i1.pdf

Centers for Disease Control and Prevention. (2011a, February 28). *CDC Information Technology Infrastructure - FY 12 Exhibit 300A&B*. Retrieved March 22, 2012, from Federal IT

Dashboard: <http://www.itdashboard.gov/investment?buscid=258>

Centers for Disease Control and Prevention. (2011b, February 28). *National Electronic Disease Surveillance System - FY12 Exhibit 300*. Retrieved March 22, 2012, from Federal IT

Dashboard: National Electronic Disease Surveillance System - Current Exhibit 300

Centers for Disease Control and Prevention. (2012a, February 22). *CDC Information Technology Infrastructure - Current Exhibit 300*. Retrieved March 22, 2012, from Federal IT

Dashboard: <http://www.itdashboard.gov/investment?buscid=258>

Centers for Disease Control and Prevention. (2012b, February 24). *National Electronic Disease Surveillance System - Current Exhibit 300*. Retrieved March 22, 2012, from Federal IT

Dashboard: <http://www.itdashboard.gov/investment?buscid=262>

Centers for Disease Control and Prevention. (2012c). *About the CDC Unified Process*. Retrieved March 10, 2012, from Centers for Disease Control and Prevention Homepage:

http://www2.cdc.gov/cdcup/library/other/about_up.htm

Decker, A., & Fitzpatrick, J. (2007). *How the CDC Enterprise Architecture Development Methodology Can Help You*. CDC.

FEA-SPP Working Group. (2010). *Federal Enterprise Architecture Security and Privacy Profile*. Washington, DC: Government Printing Office.

Federated IT. (n.d.). *Project Profile - Department of Energy (DOE) National Nuclear Security Administration (NNSA)*. Retrieved March 21, 2012, from Federated IT Corporate Site:

<http://federatedit.com/services/information-assurance/nnsa>

National Nuclear Security Administration. (2011a). *Implementation Plan 2012-2016*. Office of the Chief Information Officer.

National Nuclear Security Administration. (2011b, February 28). *NNSA ASC LLNL Sequoia Platform - FY12 Exhibit 300*. Retrieved March 22, 2012, from Federal IT Dashboard:

<http://www.itdashboard.gov/investment?buscid=571>

National Nuclear Security Administration. (2011c, February 28). *NNSA Y12 ERP - FY12 Exhibit 300*. Retrieved March 22, 2012, from Federal IT Dashboard:

<http://www.itdashboard.gov/investment?buscid=575>

Office of Management and Budget. (2008a). *Improving Agency Performance Using Information and Information Technology*.

Office of Management and Budget. (2008b). Planning, Budgeting, Acquisition, and Management of Capital Assets. In *Circular No. A-11*. Washington, DC: Government Printing Office.

Office of Management and Budget. (2011). *FY13 Guidance on Exhibit 300 - Planning, budgeting, acquisition, and management of IT Capital Assets*. Washington, DC: Government Printing Office.

The Chief Information Officers Council. (1999). *Federal Enterprise Architecture Framework*. Washington, DC: Government Printing Office.

U.S. Department of Energy. (2005). *Audit Report: Development and Implementation of the Department's Enterprise Architecture*. Inspector General. Washington, DC: Government Printing Office.

U.S. Department of Energy. (2008). *Order 200.1A - Information Technology Management*. Washington, DC: Office of the Chief Information Officer.

U.S. Department of Energy. (2009). *Information Resources Management Strategic Plan 2009-2011*. Washington, DC: Office of the Chief Information Officer.

U.S. Department of Energy. (2011a). *Department of Energy FY 2012 Congressional Budget Request - National Nuclear Security Administration*. Washington, DC: Government Printing Office.

U.S. Department of Energy. (2011b). *FY 2012 Congressional Budget Request - National Nuclear Security Administration*. Washington, DC: Government Printing Office.

U.S. Department of Energy. (2011c). *FY 2013 Summary Control Table by Organization*. Washington, DC: Government Printing Office.

U.S. Department of Health and Human Services. (2011). *FY2012 Centers for Disease Control and Prevention Justification for Estimates for Appropriations Committees*. Washington, DC: Government Printing Office.

U.S. General Accounting Office. (2011). *NNSA Needs More Comprehensive Infrastructure and Workforce Data to Improve Enterprise Decision-making*. Washington, DC: General Accounting Office.

United States Government. (2012). *Portfolio*. Retrieved March 22, 2012, from Federal IT Dashboard: <http://www.itdashboard.gov/>

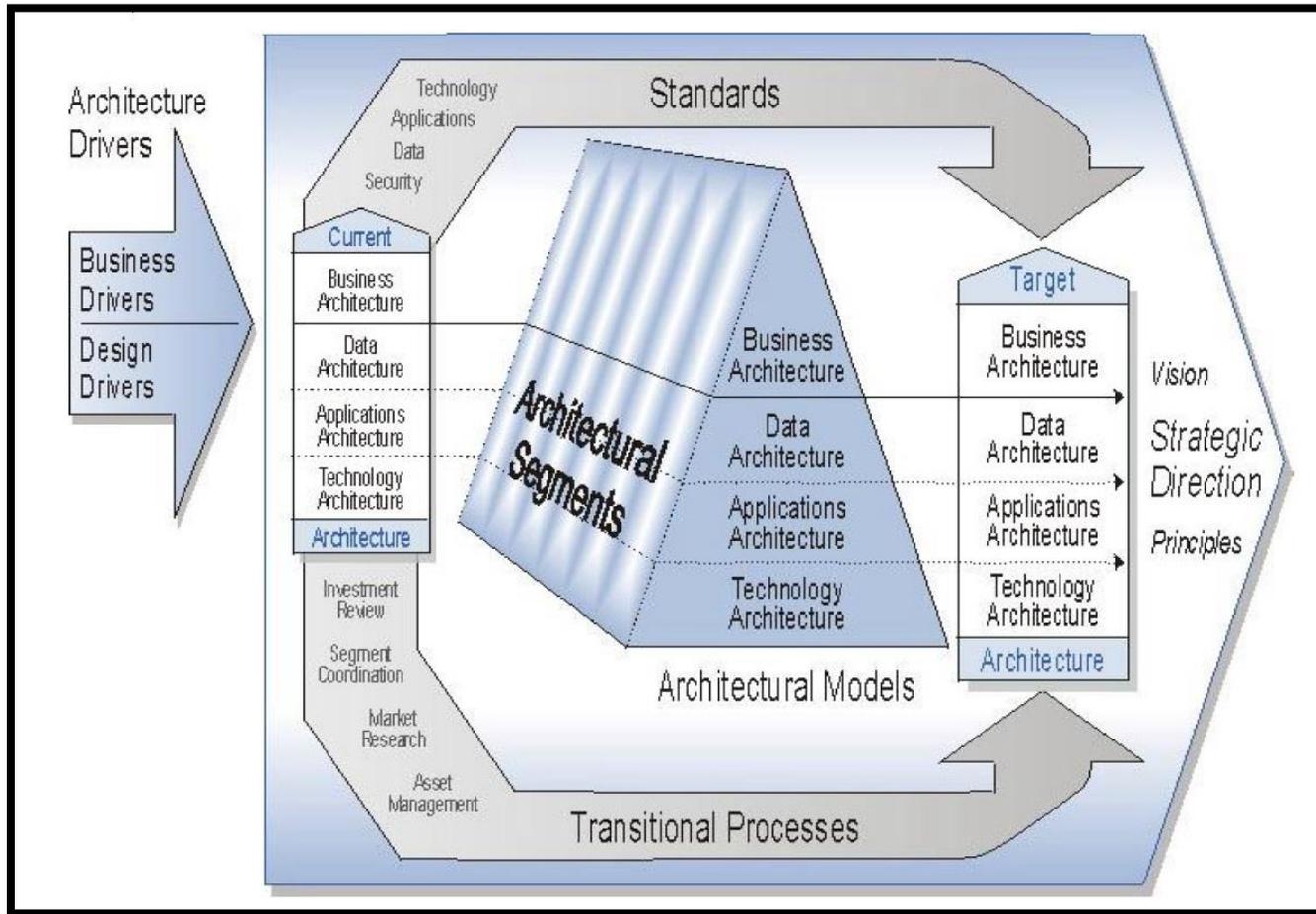


Figure 1: Federal Enterprise Architecture Framework (FEAF)

source: (The Chief Information Officers Council, 1999)

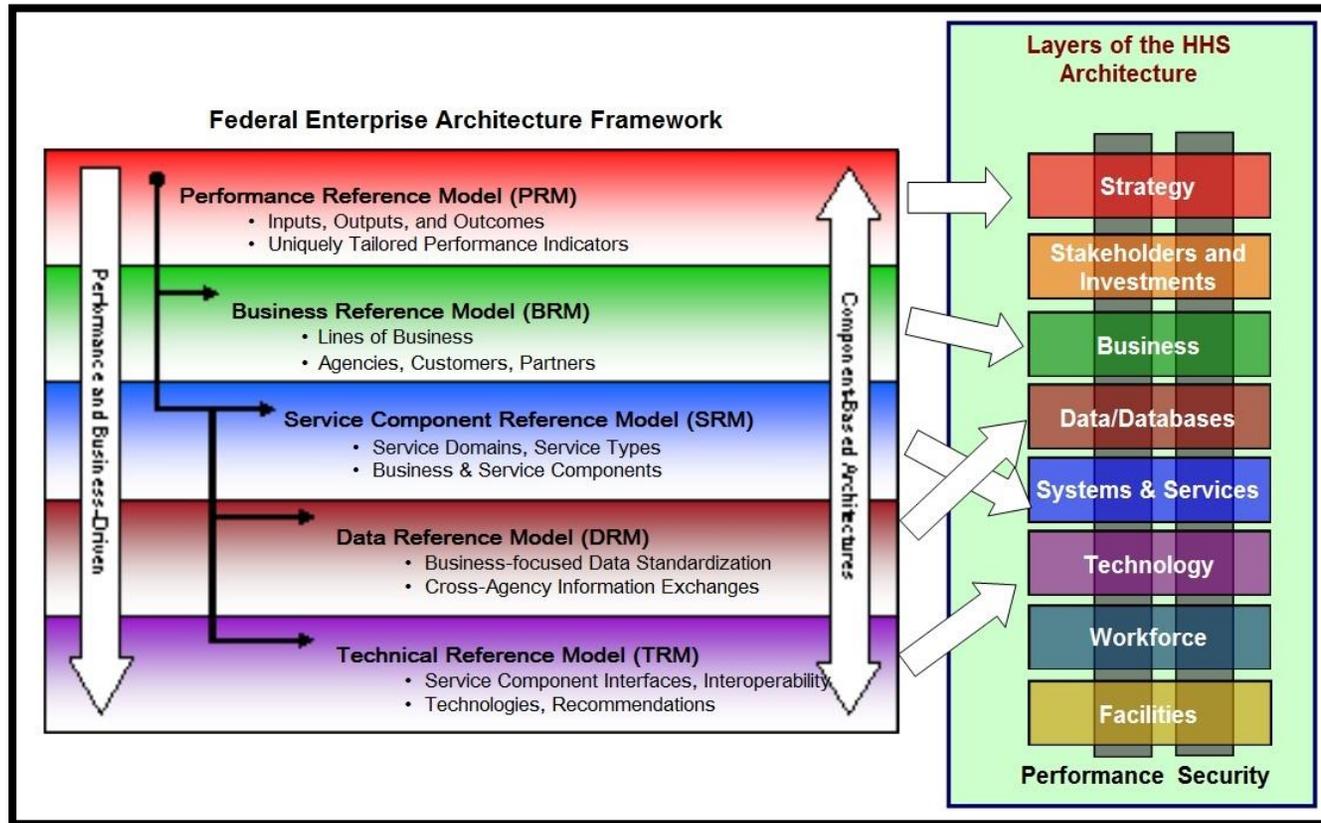


Figure 2: Federal Enterprise Architecture Framework mapping to the Health and Human Services Enterprise Architecture

Framework. Source: (Centers for Disease Control and Prevention, 2007)

About the author



Author: Christopher Furton

Website: [Http://christopher.furton.net](http://christopher.furton.net)

Certified professional with over 12 years of Information Technology experience and 8 years of hands-on leadership. An expert in cyber security with both managerial and technical skills proven throughout a career with increasing responsibility and performance expectations. Known ability to translate complex information for universal understanding. Detail-driven, results-focused leader with superior analytical, multitasking, and communication skills. Well-versed in industry best practices including Project Management and IT Service Management. Currently holding active CISSP, CEH, ITIL Foundations, Security+, and Network+ certifications.

Visit the author's blog:

IT Management Perspectives - <https://christopherfurton.wordpress.com/>

Social Sphere:



[LinkedIn](#)



[Twitter](#)



[Google+](#)



[Quora](#)



[Wordpress](#)



[Flavors.me](#)

[Flavors.me](#)



[Slide Share](#)



[Tumblr](#)



[YouTube](#)



[Pinterest](#)



[About.me](#)



[Vimeo](#)