service design collective

Defense Resourcing for the Future: Building a Strong Technical Foundation

Published March 15, 2024: Version 1
Service Design Collective, Inc.
A public benefit company
Contact: ppbe.project@servicedesigncollective.com

Table of Contents

Overview

In an ideal world, the Department of Defense (DoD) and Congress would collaborate seamlessly in real time to ensure the DoD budget and planning process would meet the immediate needs, technical capabilities, and geopolitical demands of the U.S. military. Decisions and discussions would be supported by data that served as a reliable source of truth. Questions would be nuanced and decisions would be implemented swiftly. With few structural changes since its creation in the 1960's, however, the current Congressional budgeting process struggles to meet the needs of the DoD in the 21st century.

To help resolve this disparity, section 1004 of the National Defense Authorization Act (NDAA) for Fiscal Year 2022 created a Commission to assess the Department of Defense Planning, Programming, Budgeting and Execution (PPBE)[1] process, and make recommendations for future improvements. In August 2023, the PPBE Reform Commission released an interim report containing a robust list of early recommendations that the DoD agreed to adopt.[2] The Commission's final report, Defense Resourcing for the Future[3], was published on March 6th, 2024.

The PPBE Reform Commission found that the DoD and Congress share common goals to steward taxpayer dollars and keep the nation safe, but poor communication and slow response times have strained their relationship. These fragmented lines of communication are exacerbated by a suite of obsolete, unreliable, and hard to use software. DoD has hundreds of systems that track budget-related data across a sprawling, hierarchical bureaucracy. Despite recent progress on data integration, these systems remain riddled with inaccuracies.

Meanwhile, Congressional communication is divided along House, Senate, committee, party, and individual lines. Congressional staff lack the authority or resources to maintain complex technical systems and struggle with staff turnover, leaving the Hill mired in siloed communication patterns with little cohesion. Trust has eroded between DoD and Congress in part due to the difficulties of sharing information internally, with one another, and uncertainty over the impact of greater transparency.

The PPBE process is the nexus between these two very different and equally complicated decision-making bodies. The combination highlights the worst qualities

[1] Commission on Planning, Programming, Budgeting, and Execution Reform
[2] Deputy Secretary of Defense Statement
[3] Defense Resourcing for the Future

of each. Currently, information exchange between the DoD and Congress is manual and ad hoc, consisting of email, PDFs, printed materials, spreadsheets, Word documents, phone calls, and in-person meetings. Year-to-year, very little information is recorded, maintained, or used to improve future PPBE iterations. DoD has not granted Congressional staff access to DoD networks, severely limiting options for the transfer of sensitive or controlled data. Congress reserves learnings to individual offices or committees, or keeps data behind partisan walls. Flawed technologies only add to the mistrust and confusion.

Recognizing this, the PPBE Reform Commission recommended the creation of communication enclaves to facilitate better information sharing between the DoD and Congress and help build trust during PPBE discussions.[4] In late 2023 and early 2024 Service Design Collective (SDC) worked closely with Commission staff to add supporting details and concrete next steps to the enclave recommendation. SDC reviewed the findings of the PPBE Reform Commission and other supporting materials, conducted qualitative interviews with 15 people and observed 8 hours of live and recorded product demonstrations. All participants held current or former roles in Congress, for the DoD, or at Defense-focused think tanks. Many served more than one of these roles.

The following report outlines our findings, makes practical recommendations, and suggests next steps for implementing the enclaves. Our definition of an enclave includes the digital infrastructure, software, data, business processes, service offerings, and the necessary expertise to facilitate timely and accurate knowledge and data exchange between Congress and DoD. The enclave involves technological layers, including data sources and governance, a user interface (UI), credentialing, access, and authentication processes as well as human behaviors that happen outside of technology systems.

DoD has already taken some initial steps toward sharing data with Congress by leveraging existing infrastructure and programs. Based on SDC's observations of current practices, fundamental changes are necessary before meaningful steps can be taken toward building the enclave.

Our findings include:

- A significant and widespread lack of Human-centered Design
- Poorly designed, inaccessible, and inaccurate technologies
- A lack of organization and unclear ownership around enclave development

[4] Recommendation #19 PPBE Commission Final Report March 2024

Our recommendations include:

- Assign and empower a product leader in the Chief Digital and Artificial Intelligence Office (CDAO) from the DoD whose primary responsibility is delivering the enclave
- Create a multidisciplinary integrated product delivery team staffed by DoD employees to own and build the enclave
- Establish stable multi-year funding for the development of the enclaves
- Leverage existing contracts for commercial software whenever possible, rather than pursue custom development
- Shift to a technical infrastructure that can responsibly manage sensitive DoD data on an unclassified network
- Use an authentication service and distribute Common Access or Personal Identity Verification Cards (CACs or PIVs) for credentialing
- Establish modern access controls to ensure data is protected and managed throughout the enclave
- Improve the data management and development practices of existing DoD data platforms
- Implement a single user interface to facilitate Congressional access to data
- Design and build the enclave with direct input from Congressional staffers, DoD employees, and other intended users

These recommendations are designed as a starting point for the next iteration of the enclave. They should not be understood as a completed product roadmap or delivery plan. The goal of this report is to describe the problem space and outline options for first steps. Built correctly, feedback from users will guide product decisions and will lead to a product that not only works, but is accessible, understandable, and useful.

Assumptions

This report is a snapshot in time, reflecting the realities of the DoD's budget process, software systems, and the Commission's findings. Based on the following assumptions, this report is divided into three areas of exploration; Human-centered Design (HCD), security and technology, and operations and ownership. Vast improvements across all three categories will be necessary in order to develop an enclave that improves communication and fosters trust between the DoD and Congressional staff.

Assumption 1: The needs of the enclave will change over time. Several of the Commission's recommendations, such as transforming the budget structure, would fundamentally change the enclave as a product. If accepted, those changes will take years to implement. DoD is currently attempting to implement the enclave recommendation and we assume development will continue. Building the enclave before implementing the more complex recommendations from the Commission's report will mean the enclave will be built for the current budget structure and will need to evolve alongside the implementation of the Commission's other recommendations.

Assumption 2: Advana will be a part of the enclave. Advana, short for Advancing Analytics, is a centralized data and analytics platform that provides DoD users with common business data, decision support analytics, and data tools.[5] To its credit, Advana contains a number of high quality commercial applications and digital infrastructure tools that have all been deemed secure by the DoD to manage unclassified data, controlled unclassified data (CUI), and classified data. Advana currently ingests data from over 450 DoD systems, and was mentioned frequently as the authoritative platform for analytics. It is already being used by the Military Departments for data analytics.

Current development and business practices around Advana are deeply flawed. Advana has serious usability issues, lacks sufficient data structuring and labeling, and has performance issues including, but not limited to, unacceptably slow load times and incorrect or incomplete data sets. Despite its flaws, Advana could provide the enclave with several significant benefits. Built properly, an enclave could leverage a data layer like Advana to collect information from the many systems and sources throughout the DoD and deliver it to Congress via a single user interface. Since Advana has already cleared several security-related hurdles, is being used by

[5] VOLUME 1, CHAPTER 10: Advana – Common Enterprise Data Repository for the Department of Defense

DoD internally, and has some funding, we assume it will continue to function as the DoD's common enterprise data repository.

Assumption 3: DoD will own the enclave. While the enclave focuses on Congressional needs, Congress lacks sufficient continuity, staff, and resources to develop and maintain the enclave. DoD has the expertise, resources, and ability to build the enclave. Furthermore, the enclave will contain primarily DoD data and the Department should be responsible for its management.

Assumption 4: Congress wants and will use the enclave. Many of our research participants said they wanted more access to data, but very few use the resources currently available. Staffers want their questions answered with up-to-date, detailed information. Current offerings do not provide such data. The enclave will need to address Congressional needs for it to be useful. Importantly, it will not entirely replace the human interaction needed to make complex budget decisions.

Assumption 5: User behavior and cultural expectations must change to support the enclave's success. While technology can solve many issues, there are still processes and patterns in place that must change to make an enclave successful. This includes changes in both the DoD and Congress as part of a joint effort to develop a more robust system that is responsive to user needs in both branches of government.

Assumption 6: Terminology will change. As the PPBE process of today changes and is eventually retired, the acronym will no longer be relevant. We use PPBE in this report to describe the entire end-to-end DoD financial process. The Commission has named the successor to PPBE the Defense Resourcing System (DRS). For the purposes of this report, PPBE should be understood to be interchangeable with DRS or any emerging terminology that replaces PPBE.

Assumption 7: Congress and DoD are working toward a common goal in good faith. Congress and the DoD share a common goal of keeping the United States safe. While rare individuals might act in bad faith, we assume the overall PPBE process operates in a way that preserves the integrity of the system as a whole. Nearly everyone involved in the PPBE process works as best they can through a complicated process fraught with many challenges.

Assumption 8: The first iterations of the enclave will be unclassified. There are substantial benefits to offering a classified enclave but technical, policy, and cultural barriers make it much harder to implement. Sharing any information

between DoD and Congress, even publicly available data, in a timely, accurate, and automated manner is currently extremely difficult. We focus on architecting an unclassified system first. Future efforts should strive to develop a classified enclave but the DoD should begin with unclassified data sharing.

What's Possible

The concept for the enclave is straightforward and relatively simple to imagine. Congressional staff are interested in understanding the origin and purpose of the programs they oversee. They want to follow how much money was allocated to a given program and how much has been spent to date. They want to know what was purchased, how spending relates to the end goal, and what still needs to be accomplished. Because most programs are multi-year efforts, the DoD has some flexibility in executing budgets. Congressional staff want to track if, what, and how much money has been re-programmed into or out of a budget. They also want to understand if, what, and why program objectives have changed. In addition, there are numerous program-specific details and data points that need to be shared. National and geopolitical forces may also intervene, requiring unexpected or unique data requests. Put simply, Congressional staff want to know if programs are over or under budget, succeeding or failing. If programs are not on track, they want to know why.

DoD benefits dramatically from swift and predictable budget decisions from Congress, including annual budgets, above threshold reprogramming, and new start requests. To speed decision making and reduce the vast number of wide-ranging queries from Congressional staff, the DoD can proactively provide access to a secure, controlled environment furnished with relevant data. DoD doesn't need to anticipate or answer every question. Rather, the DoD can provide enough data to answer most common inquiries, reducing the need for mundane briefings, emails, and formal requests for information. DoD can share enough budget, acquisition, and execution data to ensure that unanswered questions are narrowly tailored and well-informed. Seamless, reliable, and easily accessible data would create an atmosphere of trust and foster productive dialogue. Ultimately, with fewer and higher-quality questions from Congress, the DoD can spend more time focused on executing its mission.

DoD can share the majority of that data with Congress in an unclassified environment. Such data is not classified today and would be sufficient for Congressional oversight. Importantly, reasonable security controls and an

appropriate level of data fidelity create a manageable level of risk, making it possible for Congressional staff to access the data from their desktops via a single, intuitive user interface. They could see data based on access levels controlled by the DoD and in accordance with their Congressional role and security clearance level, which would also be managed by the DoD. Classified data would be accessible by those who need it via separate, appropriate systems. With modern data management practices in place, access to each specific element of the data could be individually controlled and every time any individual piece of data is accessed, that access would be logged. This would be much more secure than the current practice, which is heavily reliant on emailing documents and printing out paper copies for distribution.

DoD has hundreds of systems that it must pull structured and unstructured data from in order to populate the enclave. It can use a single, central data layer to extract and distribute the information. Data management rules would ensure all data is tagged and structured in a way that allows the enclave to pull from a single, authoritative source or proxy. All data and systems would report when they were last updated and when they will update next. Users with an appropriate access level would see data, those without would not.

Congressional staff would submit to a background check and the DoD would issue them CACs or PIVs. These physical identification cards would grant access to a secure, unclassified environment. An identity management system would verify identity and clearance levels would be validated by the Defense Information System for Security and related systems. Once approved, users would gain access to a commercial off the shelf software platform where they could see metrics for DoD programs of their choice as well as run unique queries.

Unfortunately, this is not how Congress and the DoD currently interact, nor is it the way the DoD has structured and organized their technology. Instead, interactions between the DoD and Congress are defined by a lack of Human-centered Design, poorly designed technologies, and unclear business organization and product ownership. While possible, change will require significant effort.

Findings

A lack of Human-centered Design

Most of the PPBE process is managed through in-person meetings, email, printed materials, and bespoke Excel spreadsheets. Budget and program data is converted to PDF and back or into other formats through multiple processes. Data is often manually retyped. The current process is inefficient, difficult to navigate, and impossible to track accurately over time. Despite the best efforts of most of the participants, it is not possible to maintain data integrity in the current system.

Each DoD program office builds and maintains internal tools for their own needs and to their own specifications. This results in inconsistent information across DoD offices. Demonstrations of these tools showed serious usability problems. Despite this, the DoD has begun granting Congressional staff access to some of these tools. Simply sharing these tools with Congressional staff does not mean Congressional staff can or will be able to use them effectively. Congressional staff have not been trained to use them nor do they have the time to learn the intricacies of every individual system to which the DoD might grant them access.

Currently, select Congressional staff have access to an enclave pilot project developed by the DoD Chief Digital and Artificial Intelligence Office. This pilot product was built using tools and data from Advana and housed on unclassified infrastructure (IL 2) called the Secure Unclassified Network (SUNet). The pilot currently contains three applications: Historical Selected Acquisition Reports (SAR), the Defense Acquisition Visibility Environment (DAVE), and Middle Tier of Acquisition (MTA) programs. Advana manages enclave pilot access via password, username, and two factor authentication code. Advana also provides a basic user interface for the pilot.

During our research, we discovered the DoD granted 12 individual users access to the enclave pilot. Only four had ever successfully logged in. To explain the lack of adoption, participants pointed to password timeouts, a lack of technical knowledge, non-existent training, and the burden of learning new programs. Others were simply unaware they had been granted access. Based on demos, we found the enclave pilot is hard to use, contains limited data, and performs poorly. Demonstrations included sizable, unexplainable errors with little recourse for confused users. Our research could not determine if anyone was still using the existing pilot in a meaningful way.

Despite the lack of adoption of earlier programs, the DoD plans to grant Congressional staff access to more tools, such as the Congressional Hearings and Reporting Requirements Tracking System (CHARRTS). DoD created CHARRTS to track deadlines and reporting requirements contained within the National Defense Authorization Act (NDAA), Defense Appropriations Bill, or other relevant legislation. Congress has requested access to CHARRTS to gain insights into how the DoD is managing Congressional requirements. DoD promised Congressional staff access to CHARRTS but has yet to deliver. Despite this, we were told that CHARRTS data will become part of the future enclave.

CHARRTS has significant usability problems, very few dedicated resources, and no HCD capacity. The future of the application is also unclear. CHARRTS is an excellent example of how simply granting access to an existing system does not satisfy Congressional needs.

Ease of use

Congressional staff have requested access to DoD systems, but applications such as the enclave pilot and CHARRTS are difficult for even experienced users to operate. When leading product demos, seasoned DoD staff struggled to interact with them. Systems returned results that were sometimes incorrect or incomplete. Even when accurate and complete, much of the information contained in these systems is not relevant to Congressional staff.

CHARRTS has many years of historical data, for example, but several participants indicated that historical data is of limited use because reprogramming changes budgets over time. Furthermore, CHARRTS contains multiple versions of the same PDF, creating a confusing collection of nearly-but-not-quite-identical documents. Without context and training, access to CHARRTS is unlikely to provide satisfactory insight into how the DoD is responding to Congressional budget requirements.

Likewise, navigating Advana requires data science skills and a deep knowledge of DoD budget minutia. It is a powerful tool for some users but for Congressional staff without such knowledge or skills, Advana is effectively unusable. Advana's potential to spin up infinite applications may make it a useful internal DoD tool, but it comes with significant risks: inconsistent taxonomy, complex and jargon-driven navigational structures, lack of useful metadata, and inaccessible user interfaces. The apparent lack of oversight creates a steep and worsening learning curve for non-expert end users, whether they are DoD or Congressional staff. Advana is designed for people who have the time and the need to become experts in the

system itself and the skill to navigate a repository of unstructured data. While it does represent a leap forward for the DoD's use of modern data tools and infrastructure, it is not designed for Congressional staff and cannot meet their needs.

User interface

Navigating the enclave pilot and CHARRTS is difficult due to poor user interface design and lack of predictable functionality. All these systems contain major user interface issues like broken features, inconsistent interactive elements, erroneous data results, and unintuitive system behaviors. CHARRTS, for example, has an extremely antiquated user interface, with small text, low contrast design elements, and older, table-style HTML pages.

The enclave pilot contains three applications, each with user interface issues. During product demos we observed low contrast colors, inconsistent button styles, unexpected animations, non-standard navigation methods, and form fields that were too small. These systems likely do not meet the Federal government's own accessibility guidelines.[6] Each application within the enclave pilot has its own look and feel, there are no consistent design patterns. What little taxonomy that exists in the underlying Advana platform is not written in plain language.[7] Instead, it uses Advana-specific acronyms and language unfamiliar to non-experts.

User feedback

Congressional staffers we spoke with said they had not been asked to provide input on what was built in the enclave pilot. During product demonstrations, the Advana team referred to user stories driving pilot functionality, but it was unclear if they had spoken to Congressional staff. Without direct input from Congressional users it is hard to know where these user stories came from. Advana has an unclear team structure and HCD capacity. Even if the Advana team has dedicated HCD resources, they are not reaching out to users in a proactive, collaborative, or productive way.

For Congressional staff to adopt and use the enclave, they will need to change their current workflows and behaviors. They will not do this with a system that is difficult to use or does not meet their needs. Building a system without their direct feedback and involvement will result in continued and additional usability issues.

[6] Section508.gov and Strengthening Digital Accessibility
[7] Plainlanguage.gov

Building trust through design

CHARRTS and the enclave pilot reinforce the distrust between Congress and the DoD through poor performance. During our CHARRTS demo, key features were clearly broken. Advanced search functionality had not worked for an undetermined amount of time. Several of the features in the search menu had been deprecated, but never removed from view. If Congress were given access to CHARRTS, it would cause significant frustration, as it did for the people demonstrating the product.

Likewise, the enclave pilot contains historical acquisition data but provides no insight into how up-to-date or accurate that data is. When the system fails, which it does, it is difficult for users to diagnose how, why, or what to do about it. During our demo, the Acquisition Budget Estimate application failed to pull data correctly, displaying an alarming $10 billion dollar deficit. No on-screen warning or explanation was available to the user. Even DoD staff leading the demo could not explain the error. Users were expected to know that the data was incorrect by guessing. Alternatively, to verify information, the user would need to reach out to a developer for support, something that was also not clear in the system. Notably, this $10 billion error occurred in a system that is currently live and accessible by Congressional staff. These types of unexplained errors sabotage user trust, reinforcing the appearance DoD is improperly tracking its spending or hiding information from Congress.

Additionally, the enclave pilot displayed extremely slow performance times, taking several minutes to complete queries and load pages. By contrast, Google considers load times over two seconds unacceptable. A 2017 Google report[8] indicated that an increase in load times from one second to three caused one third of users to abandon the system. During our demo, single pages took over five minutes to load. When asked how Congressional staff would go about reporting a problem, the Advana team advised that users would need to contact a developer to report a broken data link or understand when a data set was last updated. It was unclear in the system how staff would contact a developer.

User adoption for the pilot is low because the system is poorly designed, inaccurate, and unreliable. Users will only adopt systems they can easily use. Poor user experience practices like long load times, undiagnosable errors, and unknown data accuracy generate more questions than answers. They add frustration and time to an already difficult process which ultimately leads to distrust.

[8] Google Page Load Time Statistics

The future enclave will need to pull data at a reasonable cadence and show users system statuses in an intuitive, straightforward way. The enclave will need to deliver results quickly, ensure accuracy, and allow users to understand what they are looking at in a holistic way. It will also need to provide customer support and intuitively display error messages without forcing the user to guess meanings, gain specialized knowledge, or require developer intervention.

Poorly designed technology & security

An enclave that aims to provide information to a large group of people, including data as sensitive as PPBE information, must be built within secure and monitored infrastructure with security best practices firmly in place. It must account for security controls that protect sensitive or potentially classified information and provide accurate representation of data across security boundaries.

Substantial administrative and programmatic work has already been accomplished in this regard. The Advana team in the Chief Digital and Artificial Intelligence Office has infrastructure, data processing, and data storage tools in place. Building on the programmatic successes of Advana's existing products, contracts, data connections, and previously approved Authorities to Operate (ATO)[9] provide the best approach to the rapid delivery of a technically acceptable enclave.

CDAO's current development and delivery strategy, however, has proven insufficient to build the enclave. Initial efforts are so unstable, inaccurate, and unusable that Congressional staff have ignored or abandoned them. What has been developed so far reduces, rather than increases, trust between the two institutions.

Data access

Both SDC and the PPBE Commission's research uncovered several barriers to Congressional data access. Congressional staff need access to a wide variety of information to make informed decisions. Most of that information is sensitive and not publicly available. DoD uses Impact Levels (IL) to describe the sensitivity of their program data. To support the PPBE process, Congressional staff will need access to at least Impact Level 5 (IL 5) for CUI.

Advana currently relies on a Secure Unclassified Network (SUNet) to provide non-DoD users access to limited data. The enclave pilot is accessed through the

[9] An Authority to Operate (ATO) is given to systems that are deemed secure scoring to the Risk Management Framework. Receiving an ATO is a required, lengthy, and expensive compliance process that applies to any unclassified technology product deployed by the government.

public internet with a username, password, and a two factor authentication code. It currently contains three applications: Historical Selected Acquisition Reports (SAR), the Defense Acquisition Visibility Environment (DAVE), and Middle Tier of Acquisition (MTA) programs.

Because DoD policy states that usernames and passwords are only adequate to protect IL 2 data, the usefulness of the enclave pilot has been severely curtailed. A large portion of the budget and execution information for the DoD is held at IL 5. To access more sensitive IL 5 data, Congressional staff must often rely on classified email in a separate facility that is able to host higher levels of information. They must access secure materials through sensitive compartmented information facilities (SCIFs) or travel to secure locations like the Pentagon. Congressional staff discussed how impractical this is.

If staffers must leave the location where they do the majority of their jobs to access unclassified information, it will create undue burden. In order to get the information and context they require, they will instead resort to requests for information and additional briefings. Requests for information create duplicative and time-consuming work for the DoD. In-person briefings are extremely useful but take a tremendous amount of coordination and preparation for all parties, which is not feasible for answering one-off questions.

Even though DoD has granted Congressional staff access to classified email, the Department has not issued Congressional staffers CACs or PIVs. These physical identification cards would allow Congressional staff expanded access to IL 5 data without forcing them to resort to classified systems.

Data management

Data in Advana does not currently follow consistent standards or labeling constructs. As data is brought into the enclave, it should be labeled with metadata: information such as where it came from, when it was received, what security levels or user restrictions that data carries with it, when it expires or is no longer relevant. This is necessary to control access and properly serve data in a relevant, timely manner.

Advana gathers data from around DoD and stores it in segmented instances of Advana. If data from one version is needed in another, the data may be either fetched or replicated internally. Replication creates copies of the same data set in different locations, risking syncing and accuracy issues as those datasets age or are

edited. Advana solves the issue of each DoD component needing to implement their own data repository and tooling but their decision to create separate instances of Advana for the Services eliminates the benefits of a central platform and further isolates data into separate communities of interest.

Single platform instance

The multiple instances of Advana are managed separately, creating inefficiency. For example, a user needing to access both Army and Air Force data would need to log in to two separate versions of Advana, one for each service. Once logged in, they would have different access to different types of data in each.

These separate instances are not sitting on independent infrastructure, instead portions of the existing infrastructure are allocated to specific sets of users and only they have access to them. These instances each maintain separate access to data and separate user controls which increases the maintenance burden and complexity of the environment. Data in one instance may be pulled from a different source or be pulled at a different time. This means the buckets of data that are available to each instance are not guaranteed to be in sync with one another.

Because the sections are managed separately and data is duplicated at different times or manipulated in separate environments, a user could look up the same data point in each system and get two different results. This structure creates inconsistent results and adds unnecessary complexity to information retrieval.[10]

Ideally, a user with a need to access data from both Services would query one database, with one authoritative set of data. If their permissions were more restricted in one location, they would simply not be able to see the result of a restricted search. Such a system would be more technically efficient and prevent errors in data replication from affecting critical decision making. Implementing this change requires examining the background decision making that led to the current implementation. Further research is needed to understand and potentially change policy decisions and directives that would make a DoD-wide system more tenable.

Usage & data metrics

Based on demonstrations that SDC observed, metrics and data usage statistics do not appear to be managed in a central location on the Advana platform. This would mean there is no way to know how many times a piece of data is accessed or what

[10] PPBE Commission Final Report March 2024, "Years of Technical and Functional Debt," 105

information garners the most interest from the largest number of people. While data access may be logged, we were unable to verify that is this case.

Once Congress is regularly accessing enclave data and using it to make decisions, these types of tracking metrics will be critical to answering questions, especially those related to sources of truth and data recency. If a specific piece of data is needed every year at the same time, the enclave could track this and ensure the information is updated and accurate when it is needed most. Other metrics like usage rates and frequently accessed data sets can help drive usability improvements and puts checks in place to ensure information availability.

Unclear organization & ownership

SDC observed that many offices own their particular part of the PPBE processes but no single office or team is in charge of coordinating enterprise-wide PPBE-related systems. This fragmented approach is highlighted by many of the PPBE Commission's findings, such as inconsistent Justification Book (J-Book) writing applications. CHARRTS, for example, is a central program for assigning Congressional requirements to their respective offices within DoD. Once assigned, however, each office manages their processes separately and outside of CHARRTS. Internal to DoD, everyone is in charge of their own data and processes which leads to inconsistency across the Department.

Congress also lacks unity, splitting work across committees, parties, and chambers. This split manifests itself in many ways. Different committees use software or processes that no other committees use. The House and Senate use different terminology for the same programs or budget items and host numerous instances of the same software program. This divide is so deep that staff in different chambers cannot even look up each other's email addresses.

Additionally, DoD and Congressional systems are built and managed by disparate teams. Within the current environment, an enclave has no clear owner and no one is ultimately responsible for its success or failure. Our study participants, regardless of background, stated that improving the PPBE process is everyone's problem and therefore no one's problem. Without dedicated resources, leadership, and authority, no one will be accountable for the outcome and the enclave will likely fail.

Funding

DoD will need to leverage existing tools and contracts to make the enclave a functional tool. Though this project will be expensive and time consuming[11], it will ultimately improve how the DoD manages data enterprise-wide for itself as well as for Congress. Currently, enclave pilot efforts appear to be funded through Advana though their future funding is unclear. Individual tools such as CHARRTS have no clear budget. Because the enclave has no direct budget and necessary data is pulled from systems managed by others throughout the DoD, it is possible that the enclave will fail, or be deprioritized. The enclave needs a leader, senior support, and clear prioritization

CDAO has built multiple instances of Advana which creates separate development and support efforts for each of these instances. In general, DoD could greatly improve efficiency and cost savings through better contracting and consolidated management. Theoretically, Advana is a good place to start consolidating programs and resources, as it has with security approvals. In practice, however, Advana is unnecessarily replicating technology, effort, and costs while creating inconsistency. Based on the lack of traction gained by the enclave pilot program, the Advana team should stop its current efforts and reconsider its approach to software development, data management, and Human-centered Design.

Recommendations

Hire an accountable leader to manage this effort

Hire a single, accountable individual[12] in the DoD to take charge of the enclave product and delivery team. This person should have experience delivering technical products at scale and successfully building digital teams. A strong emphasis should be placed on non-DoD development and delivery experience. With this in mind, and to implement quickly, it is likely this person will be hired as a Highly Qualified Expert (HQE) under Schedule A or a similar direct hiring authority.

The enclave leader should be hired into the CDAOs office and be given the authority to raise any disputes to the Deputy Secretary for resolution. The Deputy Secretary's Office gave CDAO the proper authority within the DoD to remove barriers and get

[11] The Commission has estimated these changes will take between three and five years to implement. The overall cost estimate is unknown and would require additional research to determine.
[12] Digital Service Playbook Play #6 - Assign one leader and hold that person accountable

work done with a May 5, 2021 Memo[13] from the Deputy Secretary of Defense. With this in mind, the enclave team leader must have direct access to PPBE-related data across the DoD enterprise no matter where it is stored and must be empowered to make decisions that move the project forward.

This will likely be a difficult project, politically and bureaucratically. Ideally, the leader would be someone not currently employed in the DoD, and not planning to build a long-term career in the Department. Choosing a person who meets these qualifications means they will have less interest in protecting legacy decisions or their careers and be more willing to speak hard truths and make technically correct, if politically difficult, decisions.

Dedicate a product delivery team

The enclave needs an integrated product team[14] to be successful. This team should be focused specifically on delivery; releasing working software, validating with users, and iterating on learnings. Unlike tiger teams, usually composed of policy or subject matter experts, this team should develop functional prototypes and integrate feedback from users to develop the enclave, rather than rely on policy or rulemaking as their measure of success.

The product delivery team should consist of people with a variety of skill sets including front end development, back end development, data science, technical security, HCD, and product management. This team should be wholly dedicated to the enclave without other roles or responsibilities.

Members of this team should be DoD employees who would oversee the work done by both DoD and contracted employees. Team members should be mid to senior level people who have technical and government experience and understand how Congress and the DoD work. Team members should also be competent at managing existing and future contractors. Hiring inexperienced or junior team members risks spending months getting up to speed and correcting errors.

The enclave product team should prioritize HCD and focus dedicated resources on service delivery. These specialists will be responsible for making sure the product works well for intended users, bringing best practices for intuitive design to future

[13] Deputy Secretary of Defense Memorandum on Creating Data Advantage
[14] The IPT is technical in nature and distinct from the Integration Team mentioned in recommendation #28 that is tasked with implementing all of the Commission's findings, (PPBE Commission Final Report March 2024)

iterations. Without these resources, the enclave will be built based on guesses and assumptions, once again delivering a product that does not meet user needs and is therefore abandoned.

Use Human-centered Design practices

Identify and prioritize the users of the enclave, clearly define their needs and goals, and work directly with them to build the product. The PPBE process is extremely complex without the added complications of poorly designed systems. The enclave must work well for non-technical users who have little or no prior DoD experience. The product must be easy to access and intuitive to use. The product team should not make assumptions about what users need, instead relying on research, feedback, and testing to prioritize work.

Both Congress and the DoD experience frequent staffing changes, meaning some people will always be new to the process. Staff come from a variety of backgrounds and may not have technical or data expertise. The product team must work directly with DoD users, Congressional staffers, and others in Congress who support the PPBE process to validate features and measure success. The product delivery team will also need to reach out to DoD subject matter experts, including those in the Services, to learn from their processes and understand the data the enclave ingests. Since no single organization owns the entire PPBE process, the team will be responsible for stitching the pieces together through research.

Creating user feedback loops is also critical to evolving the enclave over time. As the Commission's recommendations are adopted, user needs will change and the demands on the enclave will change dramatically. Establishing HCD practices and expertise at the onset are essential to the enclave's long-term success.

Create a stable funding source

The enclave will need a dedicated budget for development and sustainment and a long-term financial commitment to address the needs of the PPBE process and its many users. Currently, the PPBE systems that would feed data into the enclave are financed in a distributed manner. Even if efforts to consolidate key elements of PPBE technical infrastructure are successful, such as developing a single J-Book writing tool or consolidating budgeting IT systems, necessary elements of a successful enclave will be spread throughout the DoD.

An enclave is, at its core, infrastructure; a place to put data that can be accessed, searched, and understood by both DoD and Congressional staff. Hundreds of systems must feed data into the enclave for it to be useful. Because data will flow from almost all areas of the DoD, we recommend creating a dedicated budget managed by the CDAO and directed by the enclave project leader. This fund will be used to develop the enclave, coordinate across the enterprise, and ensure long-term maintenance and iteration of the enclave.

Use commercial software for user-facing interaction

Use an existing, customizable commercial off the shelf (COTS) tool as the user interface of the enclave. When a system behaves in a predictable, consistent manner, it is easier to use and builds user confidence. The enclave must have an easy to use, intuitive user interface with consistent interactive elements and design patterns. The chosen interface must work in expected ways while allowing for a certain amount of personalization to match individual user workflows.

Because individual Congressional staff have unique queries, it would be difficult to build a single tool, such as a dashboard, for all users. The system must have the flexibility to make and track specific queries on a user-by-user basis. It should allow users to define the information that is most pertinent and important to them. Such flexibility will also be important as Congress and DoD implement the larger structural recommendations from the PPBE Reform Commission final report.

A COTS solution can provide a consistent look and feel to the enclave along with an interface and features that users may already be familiar with. While open source tools exist, using commercial software has the added benefit of training materials, customer and account support, and regular updates the DoD does not have to develop in-house. COTS products are easier and faster to deploy than custom or open source solutions, making it simpler to test early functionality with users. DoD, and the Advana team in particular, already have contracts and security clearances for many suitable products. They should use them.

Establish access controls & protocols

Use CACs or PIVs instead of usernames and passwords to secure system access for specifically designated Congressional staff. The first hurdle to developing a system that everyone can use is integrating with an identity provider that can meet the appropriate requirements for user authentication and authorization.

To be successful, selected Congressional staff need access to most PPBE-related data on unclassified networks without requiring new management processes or overhead. In order to provide this, the system must integrate with existing systems that maintain user accounts in order to validate that a person is who they say they are. DoD uses a single system for user identification, the CAC or PIV, that allows a user's identity to be validated by something only they have (the physical identification card) and something only they know (the personal identification number, or PIN, for the identification card). This means that when a user logs in by presenting their identification card and typing their PIN, the system can be reasonably sure that the user is who they say they are.

Throughout our research, the suggestion of giving Congressional staff CACs was the most contentious issue we encountered. While there are commercial equivalents such as hardware tokens from RSA, Yubico, or Google, the DoD already issues CACs and PIVs to users. Implementing new systems, protocols, and hardware for such a small number of users adds unneeded complexity and will cause unnecessary delay. We understand that there is additional nuance to issuing CACs or PIVs but we recommend starting with the simplest and fastest path toward establishing access controls for Congressional staff to view relevant CUI.

By issuing selected Congressional staff members CACs or PIVs, the enclave would be able to securely display information up to IL 5.[15] This would greatly increase the usefulness of the enclave over the current IL 2 pilot. It would save Congressional staff significant time and effort by allowing them to access CUI outside of a SCIF. It would also reduce the complexity of the enclave for both Congressional users and DoD technical staff.

While security background checks are required for CACs or PIVs, DoD already manages these routine requirements for hundreds of thousands of employees. The addition of a few additional Congressional staff should be easily absorbed into the technical and logistical processes the DoD facilities already take on. In many cases, these procedures may already be in place. Many Congressional staffers already have security clearances, they just don't have access to DoD IT systems.

Integrate directory services for both the DoD and Congress. After validating a user's identity, the next step is validating the user's account. In DoD, this will involve integrating with Microsoft Active Directory, the system that maintains user's

[15] Impact Levels are defined in the Cloud Computing Security Requirements Guide: DoD Cloud Computing Security

account information such as email addresses and to which organizations they belong. In Congress, this will involve integrating with multiple different user directories as each staff and committee may maintain their own infrastructure. Because most enclave users are committee staff, it may only be necessary to access the directories of DOD's four committees of jurisdiction[16], although exceptions are likely to come up. By integrating with these authoritative user directories, the system can validate that a user's identity is tied to a specific account.

Integrate with Defense Information System for Security (DISS).[17] DISS is necessary to determine what specific data a user is able to access. There are many reasons a user may be allowed to see or be restricted from seeing specific data that may include the user's organizational responsibilities, the user's security clearance, or the user's need to know. To validate this requires integration with a number of systems that include the DISS or similar systems where security clearance and background investigation information is maintained. Such systems will be able to authoritatively determine what information a user is able to see.

Leverage existing products & contracts

Implement Login.gov. The Federal government currently has identity and authentication systems in place that can be leveraged to provide authentication. Login.gov could be integrated into Advana and would allow seamless authentication using CACs.[18] This approach would offload the complexity of identity management to a trusted government resource. It could rapidly grow the capabilities of the enclave without requiring user management be a part of the enclave team's responsibilities. Given the small number of active users, it would also be less expensive than implementing a bespoke or commercial solution. While other systems may be available (e.g. Okta or ID.me), these solutions may be more costly, more difficult to integrate, and less trustworthy than the government-owned Login.gov.

Centralize support and development costs in a single Advana contract. Advana should follow contracting best practices as well as development best practices. This

[16] The House and Senate Armed Services Committees and the House and Senate Appropriations Subcommittees on Defense.
[17] In future iterations where classified program data is maintained, there may be a need to integrate with other security systems such as the Joint Access Database Environment (JADE).
[18] Login.gov Authentication Methods

will help the product be more cohesive and make the budgeting around enclave support simpler and more transparent.

Don't build custom technology. DoD has thousands of contracts that enable every kind of technology service and software necessary to deliver the enclave. The enclave should not be a custom effort. The implementation team should research existing COTS contracts and validate those solutions to decide which one is best for the functionality users need. Advana or a similar data layer solution can be used to gather and manage data from multiple sources. Avoiding custom technology will speed delivery, decrease complexity, and improve the long-term utility of the enclave.

Create a useful data layer

Use Advana as a data layer only. Any solution that is able to gather data from multiple sources and present that data with proper tagging and structure would be sufficient. For a variety of reasons, Advana is likely to remain in place.

Advana's strengths are its approved ATO, a breadth of commercial and open source software tools, and its existing data connections. Advana falls short as a user-facing system. It is especially poorly suited for Congressional staff and should not be used as a user interface. Developing the UI is a task better suited to commercial or open source solutions like a Customer Relationship Management platform (CRM). DoD should find other solutions like Login.gov to handle authentication. The data contained within Advana is useful. The user interface and applications built on top of Advana are not.

The Advana team lacks the appropriate development skill and HCD mindset to build customer-facing applications. Instead, the Advana team should focus on establishing better data collection, governance, access, and oversight controls. Improved business processes will be critical to scaling Advana across the DoD enterprise, including support for the enclave.

Implement a data strategy that is consistent across Advana. Labeling information at the data layer is a simple best practice with many benefits including security, usability, and cost efficiency. By doing so, Advana would eliminate the need to maintain separate infrastructure for different organizations. It could expose the appropriate data to each application that requests it based on what a user is approved to see rather than what system they are using to access it. All of the DoD will benefit from improved flexibility around a user's changing needs, such as when

they change jobs or responsibilities. If a user was given oversight of a new program, for example, the system could read that change and their applications would begin showing them information related to their new responsibilities. Importantly, implementing a tagging structure at this point in time will require a significant investment of resources. More research is needed to understand those costs.

Implement a single instance of Advana. The architecture and usability of Advana should be dramatically simplified. A consolidated architecture would mean fewer instances and user controls to support. By applying data controls, all Advana users across the enterprise can access information they are authorized to see through a single environment. Only those who have appropriate access to underlying data would be able to use it.

Each piece of data should have a single, authoritative location. Any time that information is needed, it should be pulled either directly from the authoritative source or, if that is not feasible, it should be pulled from a single updated source and appropriately marked as being updated at a specific time. Unfettered data replication across environments and security boundaries leads to situations in which a system is presenting data as current when it is, in fact, out of date. This may occur when multiple organizations edit different copies of the same information that are not synchronized. This means some copies of that data may no longer be up to date due to changes having been made by another cognizant organization.

Implement a data architecture that allows single user accounts across all data sets and applications. In order for an enclave to successfully bridge the gap between people, organizational silos, and data, a single set of applications should be made available. These applications should be able to fetch any data a user is authorized to see. This type of centralized approach would improve security and communication while drastically simplifying data sharing, including sharing data with Congressional staff.

In addition to reducing administrative burden by managing fewer instances of Advana, there should be more cross-organization sharing of tools and resources. This could reduce the overall cost of the contracts that are required for enclave development and support while also inspiring more creative and beneficial uses of data across the DoD. This approach also centralizes technical support services for Advana to a single organization, lowering costs, providing consistency, and improving oversight. When implemented correctly, centralized data, tools, and services is the primary benefit of Advana.

Start with higher-level data

Provide Congress with higher-level data at first. The DoD budget is made up of 48 unique investment activities spread out over 23 different appropriations and more than 1,700 distinct budget line items (BLIs).[19] Finances are passed down through the hierarchy of DoD and with every layer it goes through, budgets are split into smaller and smaller amounts. When building out the enclave, start near the top. BEgin by sharing top-level account data instead of attempting to provide specific program or project expenditures. Focusing on higher level data will allow the product team to start building more quickly, beginning with basic data and increasing its fidelity until a useful balance is eventually achieved.

Specific requests from Congressional staff vary dramatically between individuals and portfolios. Attempting to satisfy every specific query is an unnecessarily difficult task. Once users have access to data they rarely say they want less, even if they aren't using that data. Starting at a higher level would allow the product team to test out and troubleshoot integrations and show value while avoiding expensive and time consuming investments in sharing data that Congressional staff may not use. Higher level data would also help address DoD concerns about sharing too much information and inadvertently incentivising Congress to micromanage DoD projects. Lastly, if Congress and DoD chose to adopt the Commission's recommendations, high-level account data will transition more effectively into the new budget structure.[20]

Prioritize iterative changes over time

Our research showed that amongst PPBE reform experts, current and potential enclave users, and DoD staff, there is little consensus around what the most important piece of this process is or where to start. Most of our participants agreed that digital data sharing for any of the PPBE processes would be useful, but further research is needed to understand where it is most feasible to begin.

The following section highlights potential areas and data sets to build into the future enclave. These recommendations focus on modernizing whole pieces of the PPBE process to help streamline communication. Multiple process areas can be worked on at the same time, especially as data sources are added to the enclave and overlapping resource needs are identified. The most important thing is to start somewhere meaningful and keep iterating.

[19] PPBE Commission Final Report March 2024, page 69
[20] Recommendations #4 and 10 PPBE Commission Final Report March 2024

The President's Budget. Passing the President's Budget is the annual process that every agency must go through to accomplish the work of the government. Starting the enclave here would be less politically sensitive than accessing and sharing other data sets because this information is already publicly available.

The President's Budget isn't the greatest source of friction between Congress and DoD, so it is a safer entry point to establish patterns of collaboration, before tackling harder problems that require resolving security access and clearance issues.

Justification Books. The integrated product team should consider prioritizing the PPBE Reform Commission's recommendation of making the J-Books more consistent.[21] Digitizing this process and improving the massive exchange of paper would address a common complaint from Congress and Office of Management and Budget (OMB) staff.

Staffer Day Briefing Materials. Our research showed that staffer days and in-person briefings were the most useful sources of information for Congressional staff. Because DoD is essentially pitching priority programs, the information they provide to Congressional staff is generally well thought out and effectively presented. The information presented is current and the in-person exchange allows for context that converts DoD data into actionable knowledge.

These in-person sessions are supported by information compiled by DoD and provided to Congress to support these conversations. Congressional staffers rely heavily on these briefing materials and artifacts to make decisions. They find them extremely useful, collating them into binders and tracking them over several years. Some binders are passed on to others as portfolios shift, creating valuable resources that are accessible to only a few individuals.

Digitizing these briefing materials would be an excellent place to start as they present specific scenarios, use cases, and data sets. Because the Staffer day materials contain CUI, however, digitizing briefing materials would require proper authentication and security up to IL 5.

Unclassified Acquisition and Execution Data. This is perhaps the most requested place to start from an information sharing perspective. Congress wants up-to-date data on program schedules, requirements, costs, updated obligations and

[21] Recommendation #18 PPBE Commission Final Report March 2024

expenditure rates, and a plain language overview of what is bought and why. Although further research is needed to identify more specific information requirements, program acquisition and execution data seem to make up a significant percentage of Congressional budget inquiries.

This data will be the most politically fraught. In the past, DoD has been hesitant to share this information because it fears micromanagement from Congress, improper or intrusive intervention, or politically-motivated scrutiny or interference. Sharing this data requires careful consideration of the level of fidelity and frequency with which updates are made to provide a level of oversight that is constructive and meaningful. The right balance would ensure that Congress receives useful updates with relevant context while DoD retains executive authority to manage programs and make course corrections. This effort would require careful navigation of sensitive issues.

Acquisition and execution data is also likely the most technically challenging data to incorporate into the enclave, as the pilot project makes clear. Although more research is needed in this space, our initial review indicates that this data is fragmented and dispersed across many disparate systems that may be hard to identify. We do not know to what degree Advana already ingests this data. The differences in the cadence (daily, weekly, monthly, quarterly) and fidelity of data tracking is also unknown. Early examples, such as DAVE, exposed significant errors and may cause more harm than good if released or relied upon more broadly. Further research and technical investigation will be needed to understand how complex this problem is and how best to normalize data from multiple sources.

Measure success

Choose the right things to measure. The government, in general, tends to use metrics that do not accurately measure product success. Things like the number of users, quantity of data sets, and number of applications built do not indicate if these products are meeting user or Department needs. Advana has access to more than 450 DoD data sources, for example, but we know some of that data is not continuously updated or maintained. The implementation team should set success criteria based on measures related to Congress' ability to self-serve data, answer meaningful questions about the budget and programs, or track if the DoD is meeting NDAA deadlines. These, or other measures, should focus on user needs.

Advana usage metrics should become part of the data that Advana stores and manages. Strict logging and data access metrics should become part of the data that Advana stores and manages. Usage metrics should also be captured inside the enclave to provide the product team with both quantitative and qualitative data to measure Advana user behaviors. Usage metrics would allow a product team to pinpoint areas where users are gaining the most value, and where they are unable to accomplish tasks and rapidly assess system performance issues as they arise.

Where to Start

Below, we outline how the implementation team can set the enclave project up for successful delivery. This timeline includes tasks and efforts that can overlap or run concurrently.

The Commission calls for the implementation team[22] to oversee all of the Commission's recommendations, it also establishes an integrated product team (IPT).[23] The role of the IPT is to deliver PPBE technology. The IPT should include a mix of highly-skilled product experts, designers, and engineers.[24] It should also include members with specialties, such as budgeting and procurement, that help define the problem space or navigate uncertain processes or subject areas. The IPT need not be large, but should be comprehensive across skill sets that allow the team to deeply understand the problem space, resolve disputes, vet and manage contractors, review and deploy commercial products, and direct others to write code, manage data, and conduct research.

If the implementation team is motivated, the following tasks are possible:

Within 90 days

- Hire and empower an enclave product leader
- Hire or detail technologists onto the IPT
- Research existing DoD contracts for potential COTS that could be used as a user interface

Within 180 days

- Identify potential groups with which to pilot a new user interface
- Research and identify users and their specific needs
- Research and identify what portion of the PPBE process to implement first

[22] Recommendation #28 PPBE Commission Final Report March 2024
[23] Recommendation #20 PPBE Commission Final Report March 2024
[24] Digital Service Playbook Play #7 - Bring in experience teams

- Evaluate Advana capabilities as a data layer
- Identify Congressional users who will be involved in the pilot and issue them CACs or PIVs

Within the first year

- Establish identity management and data access for initial users
- Develop and deliver working software that Congress can use
- Validate data sources as authoritative and ensure proper governance and data tagging has been implemented
- Track usage metrics to show what data is being accessed and at what frequency

Beyond the first year

- Ensure the enclave is sufficiently funded and has long-term dedicated staff and contract resources
- Continue user research and integrate the outcomes into product decisions
- Establish a regular cadence and release schedule to expand both the scope and scale of the enclave
- Establish and enforce policies for data governance for the enclave

Conclusion

The PPBE Commission has released a large body of research with multiple recommendations, many of which will take years to fully implement. The enclave is only one of these recommendations but it is an essential and foundational one. Because of its unique position as a platform for communication between Congress and the DoD, an enclave offers insights into other aspects of PPBE modernization. Done thoughtfully and effectively, an accessible, user-friendly enclave will ease tension, build trust, improve cooperation, increase transparency, and accelerate decision making. Done poorly, it will exacerbate existing frustrations.

One of the challenges with the PPBE Reform Commission findings is deciding where to begin. Many of the recommendations contained in this report may change depending on what PPBE Commission recommendations are implemented and in which order. Enclave development must also take the other Commission recommendations into account. For example, budget structure transformation could actually ease development requirements for the enclave, if done during early stages of development. If done later, it could create significant disruption. Either way, the development of an enclave will change dramatically throughout the process of implementation. It should be approached as a long-term, iterative process and should be staffed and funded appropriately. Once established, it will need sustainment to ensure it remains relevant.

Early efforts to centralize acquisition data suffer from a lack of leadership and accountability. The enclave pilot's dismal performance reflects the absence of both. To be successful, the DoD should assign a single, accountable person to lead development. They should have open access and the authority to coordinate data across the DoD enterprise. They should have enough budget to assemble an internal team of experts in product delivery and a guarantee that sufficient funding will be available to maintain the team and leverage existing contracts.

Built correctly, the enclave will help DoD reorganize and restructure its approach to data management. Organizationally, Advana has many advantages and several unrealized benefits. Good work has been done to centralize tools and security approvals but its implementation is unnecessarily complicated. Advana appears to lack oversight and organizational principles. Development is unconstrained and unfocused, at least in regard to the PPBE process. Significant effort will need to be made to centralize, restructure, and effectively reorganize and manage PPBE data. The current practice of maintaining multiple instances of Advana and replicating data has serious and negative implications. Data-driven decision making is not

effective if the data is unreliable. At best it leads to waste. At worst, it could affect critical, operational decision making. Issues like slow load times may seem trivial but will lead to system abandonment, squandered effort, and distrust. There is no point in building software that no one uses.

DoD should strive to provide Congressional staff with a single user interface that has flexibility for staff to create unique queries. That user interface should reference accurate, authoritative, and timely data. Enclave users should know when data was last updated, know when it will be updated next, and be alerted to any data that is not loading correctly. Data need not be provided in real time nor must it be comprehensive. Setting unrealistic expectations will lead to unrealized results. Instead, DoD should learn from Congressional staff and provide data that is relevant, authoritative, easy to access, and current enough to be useful.

As a north star, it is important to keep in mind that Congressional staff don't want data. They want knowledge. Knowledge requires context that data alone cannot provide. DoD cannot understand these needs without working closely and routinely with Congressional staff during development. The enclave should be approached as a solution to a communication problem rather than a technology problem. Digitizing the current, fractured communication patterns has led to useless, fractured technology. Solving the communication problem, on the other hand, will lead to simple, intuitive, and informative technology.

A large complex system simply cannot make decisions nimbly without data. Ultimately, a well-designed, properly executed enclave will be the technical foundation for change and may prove to be critical in restoring trust and improving collaboration between Congress and the DoD.

Acknowledgements

We thank the Federation of American Scientists (FAS) for sponsoring this effort and supporting our work; in particular Joshua Marcuse, Dan Correa, Aleksandra Srdanovic, Jon Wolfsthal, as well as Thomas Kalil, of Schmidt Futures. FAS's dedication to PPBE reform highlights how important this work is.

We thank the PPBE Commissioners and staff, particularly Lara Sayer and Caroline Bledsoe for their generous support, time, and resources. The work the PPBE Reform Commission has done is tremendously valuable to the nation. Our report focuses on only one part of an extremely complex set of recommendations and their research in this space has been expansive.

We thank our research participants for their generous time and insights. Without them we could not have created this work.

Thank you to our early readers for their help in making this report comprehensive, readable, and accurate.

Appendix A: References & Links

- Acquisition Research: Creating Synergy for Informed Change - Eric Lofgren
- Commission on Planning, Programming, Budget, and Execution Reform website
    - Deputy Secretary of Defense Kathleen Hicks Statement on the Release of the Commission on Planning, Programming, Budgeting, and Execution Reform Interim Report
    - Interim Report - August 2023
- Competing in Time: Ensuring Capability Advantage and Mission Success Through Adaptable Resource Allocation - William C. Greenwalt & Dan Patt
- Defense Management: DOD Should Collect More Stakeholder Input and Performance Data on Its Congressional Reporting Process - GAO
- Digital Service Playbook Play 6 - Assign one leader and hold that person accountable
- Cloud Computing Security Requirements Guide
- Advana – Common Enterprise Data Repository for the Department of Defense - DoD 7000.14-R Volume 1 Chapter 10
- DoD Planning, Programming, Budgeting, and Execution (PPBE): Overview and Selected Issues for Congress - Congressional Research Service
- Financial Management Regulation Volume 1, Chapter 10 - Common Enterprise Data Repository for the Department of Defense
- How Much Is Enough? Shaping the Defense Program, 1961-1969 - Rand Corporation
- Login.gov Authentication Methods
- Memorandum for Senior Pentagon Leadership Commanders of the Combatant Commands Defense Agency and DoD Field Activity Directors: Creating Data Advantage
- Navigating the Billions A Beginner's Guide to the Defense Budget - Molly Parrish
- Page load time statistics - Think with Google
- Plainlanguage.gov
- Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy - National Institute of Standards and Technology (NIST)
- Section508.gov
- Strengthening Digital Accessibility

Appendix B: Glossary of Terms and Acronyms

Advana: Advancing Analytics, a centralized data and analytics platform that provides DoD users with common business data, decision support analytics, and data tools

CHARRTS: Congressional Hearings and Reporting Requirements Tracking System designed to track deadlines and reporting requirements contained within the NDAA, Defense Appropriations Bill, or other relevant legislation

COTS: Commercial off-the-shelf software, any ready-made software that is available to the public to purchase, license, or lease

CRM: Customer relationship management program, any program that provides a user interface and data tools to manage and track user interactions. Examples include Salesforce, ServiceNow, and Microsoft Dynamics.

CUI: Controlled unclassified information is any information that is not classified but still requires higher levels of protection and control than publicly available information.[25]

Enclave: A broad term that includes the digital infrastructure, software, data, business processes, service offerings, and necessary expertise to facilitate timely and accurate knowledge and data exchange between Congress and the DoD.

J-Books: Budget justification books are budget documents that contain information about the specific budget items such program element identifying code, cost, description, schedule, and capabilities.

PPBE: Planning, Programming, Budgeting and Execution, the current process for allocating and using money throughout the DoD.

SUNnet: Secure Unclassified Network, is a platform for sharing unclassified program, information, and collaboration tools with internal and external partners.

[25] CUI Categories - National Archives

Appendix C: Impact Level Comparison

This chart is from Department of Defense Cloud Computing Security Requirements Guide Version 1, Revision 4: https://dl.dod.cyber.mil/wp-content/uploads/cloud/zip/U_Cloud_Computing_SRG_V1R4.zip

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	CSP PERSONNEL REQUIREMENTS & INVESTIGATION EQUIVALENCY
2	PUBLIC	FedRAMP Moderate Baseline (MBL)	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical Public Community	Tier 1 (T1)
4	CUI (FOUO, PII, PHI) or Non-CUI	Level 2 + CUI-specific tailored set OR FedRAMP High Baseline (HBL)	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Limited "Public" Community Strong virtual separation between tenant systems & information	US Persons ADP-1 (IT-1) Tier 5 (T5) ADP-2 (IT-2) Tier 3 (T3) Non-Disclosure Agreement (NDA)
5	CUI (FOUO, PII, PHI), U-NSI/NSS	Level 4 + NSS-specific tailored set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Federal Government Community Dedicated multi-tenant infrastructure physically separate from non-Federal systems Strong virtual separation between tenant systems & information	
6	Classified SECRET NSS	Level 5 + Classified overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNet DIRECT with DoD enclave connection approval	Virtual / Logical Federal Government Community Dedicated multi-tenant infrastructure physically separate from non-Federal and UNCLASSIFIED systems Strong virtual separation between tenant systems & information	US Citizens with favorably adjudicated T5 & SECRET clearance NDA