How Enterprise Architecture and a Service Oriented Approach Can Solve Architectural Issues

at the Department of Justice's Criminal Division

Master of Science

Software Design and Programming

Will Pacheco

University of Denver University College

November 10, 2019

ICT 4010: Enterprise Architecture

Professor Steven Else

Dean: Michael J. McGuire, MLS

Table of Contents

Executive Summary

The Department of Justice's Criminal Division (CRM) contains fifteen sections tasked with the responsibility of "overseeing criminal matters as well as certain civil litigation" (US Department of Justice 2017). Currently, the government is mired in legacy information technology and services that have little to no communication between departments, even when doing so would be to the benefit of all parties.

Security is an ever-present concern as aging programs are vulnerable to cyber-attack. Fortunately, the need to modernize and a realization of benefits of the implementation of best practices from Enterprise Architecture can be realized to provide solutions to the challenges and difficulties facing the Division. New goals include the creation of a common core of data that can fuel multiple, independent but related modular applications. This could also help create responsive, communicating IT services that respond to needs with secure, modern initiatives that are easily shareable between departments rather than being walled off in information siloes.

To succeed will require overcoming decades old cultural hurdles between the manifold agencies as well as budgetary constraints and plain old resistance to innovation. Additionally, Service-Oriented Architecture and Web Services provide quick and easy application stop-gap solutions to many of the issues plaguing CRM – in part by providing an example of what an Enterprise service can look like. In the end a secure, modern, agile IT department can best support the mission of the Justice Department to fight and prosecute crime and aid this historic institution in continuing its work of serving the citizens of America.

Vision of Architectural Success and General Background

The Justice Department has a problem—specifically with outdated infrastructure in an ever-evolving technological world. The current environment at the Department of Justice, and indeed, much of the Federal Government, is shaped by decades of development, an increasing set of challenges and complex responsibilities, limited resources, and outdated business processes lacking an overall strategy (Wagner 2007). In order to become a more lean, effective tool in the fight against crime, the Criminal Division must fully embrace and implement the principles of Enterprise Architecture. Within the realm of Information Technology, the mission is to "provide innovative, high quality, and secure IT capabilities to enable" the mission of the Criminal Division and its Sections (US Department of Justice 2019, 3).

To start, this paper will describe issues across the Division that put up challenges and roadblocks to realizing this mission: legacy systems, lack of governance, siloed business processes and information sharing, disparate technology systems developed before and after the implementation of a formal information technology strategy, budgetary shortfalls, security concerns, and an immature application of Enterprise Architecture. EA integration is an important aspect of DOJ strategy in order to provide a comprehensive, integrated, and scalable framework (The White House Office of Management and Budget 2012, 21). As such, the challenges facing the Division threaten to thwart that mission.

The Criminal Division is currently heading in the right direction through incremental change and continued implementation of FEAF and Department policy. The Office of Administration, often acting through Information Technology Management, continues to show

immense growth at delivering value to the Division, through the implementation of Enterprise Architecture frameworks and Service-Oriented Architecture at all levels of scope.

This paper will argue that architectural success for the Criminal Division means improved technological access and services for the legal and administrative teams overseeing justice and enforcing the country's laws. To do so, requires the minimization, and overcoming, of the challenges outlined above, as well as intuitive application of solutions, new technologies and paradigms. To reach that goal, necessitates a continued implementation of Enterprise Architecture principles through Federal Enterprise Architecture strategies and a pivot in technology services towards a Service-Oriented Architecture. Additionally, it will require a capitulation of authority to Justice Main where applicable and appropriate for the purposes of architectural integrity, and to maintain a strong foundation for execution.

The vision of success is fully realized when leadership is able to implement change and not only provide solutions to these challenges, but apply a transformation across the division with the successful application of new Service-Oriented Web technologies. These will provide a responsive, holistic, and robust set of application services. These services should, and will, provide the framework and opportunity for sections, and the Division as a whole, large-scale information sharing (sometimes referred to as "integrated justice") (Justice Information Sharing 2005, 3). Additionally, the systems enabling this information-sharing, will provide common core accessible data for customers (those served by ITM) and the future ability to establish modular (independent but communicating) IT applications. This would achieve strategic agility and the highest level of architecture maturity (Ross, Weil, and Robertson, 77).

Major Architectural Issues

The Department of Justice's Criminal Division has successfully served American society, prosecuting criminal acts across the country since its formal inception in 1919 (US Department of Justice 2019). At one-hundred years old though, it is not just an organization, it is an institution. As such, the culture and business processes of the institution are hierarchical and at times, entrenched in different periods of time. This presents functional challenges to an Enterprise Architect implementing modernization efforts across fifteen sections, each with their own cultures, leadership, legal processes, and offices across the country.

A history of siloed work between the sections of the Department of Justice has resulted in a multitude of disparate systems that are not well-documented and lack transparency even between leadership of the sections. Unfortunately, this atmosphere has resulted in many similar or duplicative legacy systems of varying importance and use. Also, due to a lack of transparency and governance, several expensive, time-wasting projects have been supported for systems that do not have a high rate of use or priority, and have not brought data together to an "optimized core" level of architectural maturity.

In the context of Service-Oriented Architecture, the Department has actually long provided Service-based information technology, albeit, without a clear idea of how to integrate with Enterprise Architecture principles. The SOA that is being utilized has survived in bits and pieces despite the challenges facing the Department. SOA should be utilized as a means of ensuring "performance and availability" beyond the individual products offered (Heffner 6). As

a means of providing a solution space, it is not quite where it needs to be. A few of the challenges facing the Division's SOA are:

Legacy Systems Challenges

- Critical legacy information technology systems at the Department of Justice are costly to maintain, present compatibility issues, and are a risk to system security.

Cultural and Process Challenges

- Each section within the Department has unique processes and cultural expectations for information technology applications that sometimes come into conflict.

Knowledge, Information, and Data Challenges

- Knowledge, Information and Data ("KID" Stuff), is often out of date, unspoken, and/or unwritten. Governance and best practices for codifying, capturing, and storing tacit knowledge, is virtually non-existent.

Cost and Budget Challenges

- Budget constraints hurt efforts to modernize, and present difficulties implementing new architectures. If overcome, this would provide immediate relief to Sections' needs and prevent silos from forming.

Security Challenges

- Security is a primary concern at the Department and continues to present hurdles as the Division attempts to modernize and provided support for IT professionals, legal experts, and administration staff to work remotely, wirelessly, and through the web.

Enterprise Maturity Challenges

- The Department of Justice employs an architectural maturity level of Standardized Technology. A lot of hardware and systems are used to produce solutions for varying Sections, resulting in disparate data sources and one-off, needs-based applications.

Implementation of FEAF and SOA

A successful organization is only as good as its strategy, and fortunately, the Department of Justice has one. The Federal Enterprise Architecture Framework provides guidance for implementation of Enterprise Architecture strategies and solutions. Additionally, it is the policy of the Department of Justice "and its components plan, acquire, manage, and use information technology (IT) and information in a secure manner that enhances mission accomplishment, improves work processes and employee productivity, provides sufficient protection for the privacy of personal information, promotes citizen-centered electronic government, and complies with all applicable federal laws and directives" (US Department of Justice 0903 2016, 8).
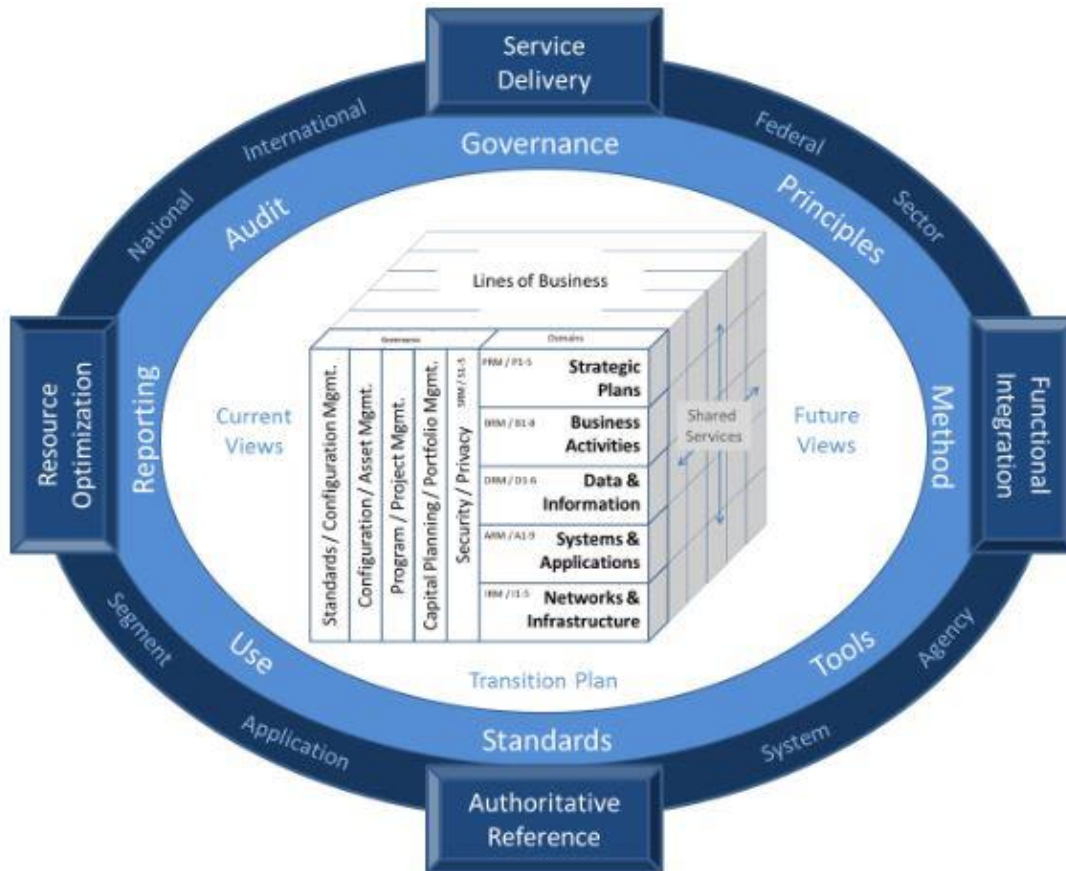
Figure 1 - Idealization of FEAF implementation (The White House Office of Management and Budget 2012, 57)

The Department of Justice Main provides its own information technology strategy that focuses on four main goals to help achieve desired outcomes.

- Continuously Improve Service Delivery – Establish reliable, resilient IT services that increase communication and collaboration through intelligence and automation (US Department of Justice 2019, 4).

- Effectively Invest in Technology – Standardize and simplify technology through shared services and strategic sourcing, while leveraging IT governance and collective decisions (US Department of Justice 2019, 6).

- Protect Critical Mission Assets - Protect assets through "continuous monitoring, automated incident response, centralized identity management, and resilient systems" (US Department of Justice 2019, 8).

- Build Innovative Capabilities – Modernize and future-proof technology through mobile-access solutions, machine-learning, reliable data, and advanced analytics (US Department of Justice 2019, 10).

Responding to the unprecedented rise and growth of consumer-level technology in mainstream culture, employees and users of federal information systems, both internal and external, increasingly expect more robust, responsive, and holistic applications that match or exceed consumer technology. As a result, the need for "faster delivery of public services and better insight into the status of their requests" becomes a necessary component of both existing and future information systems (Janssen and Cresswell 2005). Requirements for achieving this end contains artifacts, templates, security, data management, and evaluation criteria (US Department of Justice 0903.02 2016, 6). Enterprise Architecture Integration in the federal sphere, though, is a massively complex undertaking, seeking to link siloed systems for greater leverage across the Division and Justice community (Janssen and Cresswell 2005).
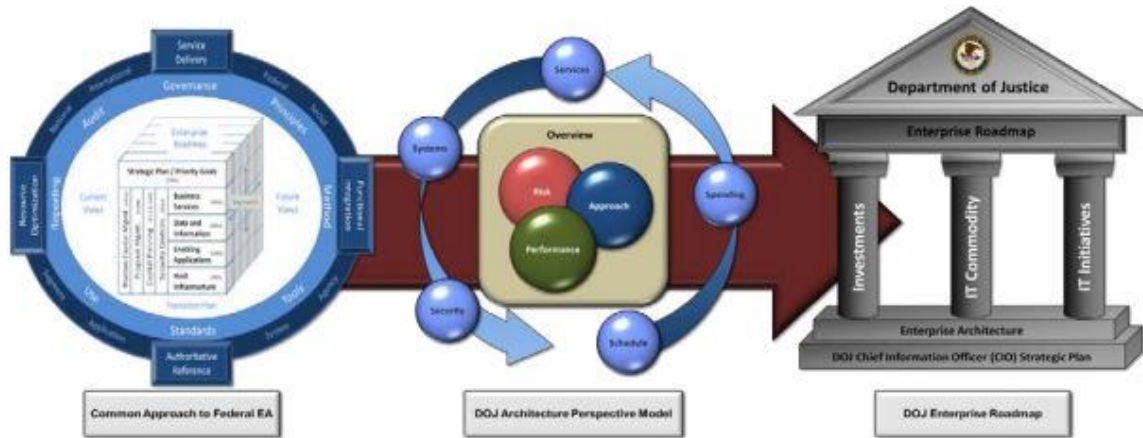
Figure 2 - DOJ Structured Approach (US Department of Justice 2016, 47)

Currently, the Department of Justice seeks to address the problems of the future and provide improved accessibility to products, services, and applications at all levels of scope through compliance to Enterprise Architecture initiatives and recommendations from Justice Main and other federal leadership bodies. From updating and replacing legacy systems to improved data management and building a strong coalition, implementation requires innovation, protection, sound investments, and continuous improvement. Understanding the goals, challenges, and vision is integral to achieving the missions of the Federal Government and the Department.

Casing Legacy System Issues

Agencies across the federal government have reported that "legacy IT investments were becoming increasingly obsolete" and that using unsupported operating systems and components will "create security vulnerabilities and additional costs" (US Government Accountability Office 2019, 8). The Department of Justice has three identified legacy systems aged 21-49 years with the highest risk determination being High and a minimum mission

criticality level of Moderately-High (US Government Accountability Office 2019, 37).

Additionally, there exist several other systems that provide web and data services within the

Department that do not fall under the technical definition for legacy. These systems are not as

old or as critical, but must be replaced, upgraded or absorbed by other systems in order to

prevent them from becoming high risk in the near future. For the purpose of this analysis, they

will be considered legacy as well.

To update these and seal the security gaps, innovation will have to overcome tradition.

"Never touch a running system" is a piece of advice often stated regarding IT infrastructures

(Bente 277). Another adage along the same lines is "if it ain't broke, don't fix it." Building on a

legacy system, though, can create problems for an organization trying to modernize and remain

adaptable to changing trends and emerging technologies. Eventually this leaves the

organization paying vast sums of money maintaining an inverted house of cards. The

architecture as a result is slow and lumbering and only as agile as its slowest pieces.

Additionally, maintenance costs associated with antiquated systems are "significant" (The

White House Office of Management and Budget 2012, 201). In order to meet architectural

security requirements, remove dependencies, reduce impact to the budget, and ultimately

provide modern Software-Oriented Architecture applications, the legacy systems must be

appropriately handled.

A Case for New Cultural Drivers and Process Changes

"Knowledge Islands can be fatal." The failure of the US intelligence community to spot

the 9/11 attacks in advance, were a direct result of agencies' reluctance to share information

except on a "need-to-know" basis (Bente, Bombosch, and Langade 2012, 270). Today, the

Criminal Division's fifteen sections operate in much the same manner. They are not in

competition, but their data and strategies are often hidden from one another. In many

instances, leadership in some sections actively refuse to modernize their business processes –

instead preferring to rely on the same methods that were used over thirty years ago, before the

widespread use of computers. These sections, at most, may send information over email, but

do not offer a way for actively sharing their insights, guidance, or experiences.

The variety of section requirements at varying levels of technical competencies, results

in many custom, tailor-made application solutions for each section. Some sections run their

own websites for instance, while other sections rely on ITM to build a website or application for

them. The data between these sites and applications are not shared in any way because they

do not exist within the same ecosystem and so do not share a common core.

Part of the problem is a cultural resistance to change that needs to be overcome by

involvement and agreement between section leadership. Information Technology solutions

need to present themselves as solutions to a problem rather than new for the sake of new.

Previous attempts from ITM to provide one-size-fits-all solutions were rejected by the sections.

Individual sections and the Criminal Division as a whole, must identify drivers, assumptions, and

constraints to solve the problem of legacy conditions and attitudes (The White House Office of

Management and Budget 2012, 77). Doing so will be a first step in modernizing and assimilating

to EA maturity and lay the groundwork needed for SOA.

Casing Knowledge, Information and Data Improvements

As mentioned above, "knowledge Islands can be fatal." Tying into the need for cultural and process changes, is Knowledge, Information, and Data ("KID" Stuff). KID stuff is the lifeblood of the Criminal Division and is without a doubt, the most important asset or currency the Division deals in. Legacy security protocols and applications, as well as existing, legacy attitudes, prevent data from being shared easily across agencies. For example, despite the Criminal Division often needing to work closely with the Federal Bureau of Investigations, there exists no easy link between the two.

This is not to make a case for opening up required boundaries, but to identify boundaries that exist that limit necessary KID sharing. The current architecture makes implementation of data sharing and implementation of SOA difficult. Currently it requires the execution of "interagency agreements or memorandums of understanding (MOU)… as long as there is a direct system-to-system connection and parties are willing to enter into agreement, data access is granted. But this model is time- and resource-intensive; limited in scope, application, and efficiency; and approaching obsolescence in the face of increasing (and increasingly complex) information needs" (Justice Information Sharing 2005, 3). The complexity and time-consuming nature of this process often results manual work-arounds (simply contacting those with knowledge of the information), or avoiding/abandoning useful projects and attempted links altogether. From personal experience, an MOU can take *months* to *years* to establish, a period of time where another solution may make itself available.

Identification of all structured data sources and collaboration between sections will be necessary for implementation of EA and SOA goals. Boundaries must be modified to fit with a new architectural standard that include strengthened IT infrastructure to leverage identified opportunities for sharing.

A Case for Smarter Budgeting

Modernization is a risky, expensive venture, especially when existing systems lack a firm foundation and grounding in Enterprise Architecture and appropriate governance. Complexity and outdated architectures have not added to the value of the Division. The positive net effect of reductions in operational redundancy and legacy systems results in increased available cashflow and lower IT costs overall (Ross, Weil, and Robertson 2012, 11). Enterprise Architecture offers the tools necessary for accomplishing the budgetary freedom that is so desperately needed and the Division should implement metrics to measure the results and outcomes of EA (US Government Accountability Office 2011). Additionally, solutions must be provided to the business cases listed above – as solving those issues will ultimately free resources and time in the future as well.

Related organizations that build IT capabilities and who leverage those capabilities "in ways that are both visible and measurable" within the scope of the Enterprise Architecture, are in a position to save money (Ross, Weil, and Robertson 2012, 194). As a reference, the Department of Homeland Security implemented metrics to measure its implementation of Enterprise Architecture, and saw $631 million in "cost savings or avoidance in fiscal years 2012 through 2016" (US Government Accountability Office 2011). That is a savings of approximately

$160 million per year. The Criminal Division is capable of seeing similar savings and more when approaching the budget in a smart and measured way through the use of Enterprise Architecture methods and Service-Oriented Architecture for applications.

Many of the other aforementioned implementation cases will provide budgetary benefits as well. As architectural changes are applied, savings and benefits across all identified challenge areas are increased.

Casing Security Risks

Permeating all levels of the architectural structure is security. At the Criminal Division, and throughout the Justice community, security is at the top of the list of concerns, especially when dealing with sensitive prosecutions and other legal investigations. The security risks facing an EA and SOA implementation stem from both foreign and domestic sources. In 2018 there were 31,207 identified security incidents levied against federal agencies and stemmed from improper usage of agency resources, web-based attacks, email/phishing scams, physical loss or theft, and many other unidentified attack vectors (US Government Accountability Office 2019). Frighteningly, these are only known attacks. There are likely many more incidents that go unreported or unidentified. The risks pose immense threat to the well-being of the country and the ability of the Division to perform its duties.

Fortunately, there are a number of controls that help to identify and reduce risk to acceptable and manageable levels. The Federal Enterprise Architecture Framework identifies four such strategies for reducing risk (The White House Office of Management and Budget 2012, 55):

- Mitigate risk through hardening software and implementing firewalls to close back doors. Controls for which are to be decided by and tailored to an organization's specific needs and requirements.

- Avoid risk by using software and systems that do not have known security vulnerabilities, carefully filtering and providing solutions to customers that are not provided by foreign entities or questionable vendors.

- Transfer risk of applications and systems to outside vendors. Essentially, outsource certain Information Technologies that are not part of the core competencies of ITM to professional services that excel at the particular infrastructure or platform (for example: cloud services, platforms as a service, security protections).

- Accept reasonable levels of risk. The only safe environment is in a bubble – don't let security be the bottleneck.

The importance for security cannot be overstated and these recommendations are suggested at every level of the Enterprise Architecture. Enterprise IT systems and services must be "designed and implemented in accordance with Department IT standards and technology direction" and "aligned with the Federal Enterprise Architecture framework" (US Department of Justice 0903.02 2016, 6). Addressing security concerns promotes interoperability of, and standardizes and consolidates, security capabilities (The White House Office of Management and Budget 2012, 55). Defining these security concerns and implementing measures to protect Division systems not only protects data from accidental and malicious leaks, but also protects resources in the long-term by preventing costly damages from successful attacks and damaging intrusions.

A Case for Enterprise Architecture Maturity

Enterprise Architecture integration requires a portfolio of techniques and strategies to achieve success (Janssen and Cresswell 2005). The portfolio includes systems, application components and interfaces, which are identified through the Application Reference Model. The Application Reference Model can be defined by application services "offered with a Service Oriented Architecture (SOA) and should facilitate shared services and interoperability" (The White House Office of Management and Budget 2012, 184). Bringing these components together reduces redundancies and provides the basis for sharing and reuse, the foundational principles of architectural maturity.

Architectural maturity is a concept that as an organization builds out and adopts their enterprise architecture, the business processes and IT solutions transform to where they can offer greater value at the expense of local autonomy (Ross, Weil, and Robertson 2006, 71). As mentioned, knowledge management and business processes are challenges to overcome. These challenges tie directly into the challenge of achieving architectural maturity and the implementation of Enterprise Architecture principles against those challenges, allowing for maturity growth overall. Analysis of business and data environment, within the "context of the strategic improvement opportunities," is required to make data adjustments and fulfill project requirements and overall EA vision (The White House Office of Management and Budget 2012, 112). Specifically to the Criminal Division, there is a need to expand the power of Information Technology Management, through the Office of Administration. This means taking a greater role in certain design process decisions from unit leaders in order to establish a more cohesive whole (Ross, Weil, and Robertson 2006, 77).

This is a formidable challenge for information technology, who, following analysis, must work with planners to actually implement a template for digitizing reusable data, consolidating existing digital data, and transforming it into an optimized core. They are then responsible for building out business applications that are capable of leveraging that core. In the end though, the Division will be able to implement an efficient application offering, centered around a thick core of data and services, that is modular in nature and is capable of responding quickly to changing conditions in the federal space (Ross, Weil, and Robertson 2006, 79). The process to Business Modularity will be incremental, and requires leveraging implementations of EA principles across the board in knowledge management and cultural shifts.

Summary of Implementation: Main Points

This paper covered several points in the struggle to bring the Enterprise Architecture of the Criminal Division into the present day and the future, which is where it should be. To summarize the main points of an Enterprise Architecture implementation to overcome challenges, refer to the bulleted list below:

- Identify and plan for retirement and replacement of legacy systems

- Involve Section Leadership and build Collaborative Agreement

- Modernize Business Processes and governance

- Identify points of data application system redundancies

- Identify points of possible KID sharing and structured data sources

- Implement KPI tools for metric tracking across all architecture plans

- Study metrics for Enterprise Architectures to track and improve budget

- Define security concerns for new enterprise endeavors to mitigate risk

- Plan for an optimized core for improved application and process efficiency

- Plan for incremental improvements to core to eventually leverage business modularity

The Business Case

Justification for Enterprise Architecture Integration and Software-Oriented Architectures exist of course in the responsibility of agencies and the Division to comply with federal guidance. That, while being an official driver for implementation, does not address the myriad needs of the responsibility of the Department to provide modern solutions to modern problems. EA and SOA provide the architectures and guidance necessary for identifying the needs and providing the tools to solve the challenges facing the Division. Implementation brings together data, metrics, strategy, governance, and fiscal responsibility across the Divisions' sections. Federal agencies need a strategy that will not only catch them up to 21st century businesses and public expectations, but give them the momentum to maintain that ability.

Risks to the Division are stalled initiatives and data loss, if implementation is not done or is unsuccessful. A migration towards a fully realized Enterprise Architecture, could take years due to institutional resistance and inertia. The technical and strategic challenges to implementation are immense and require much planning, unity-building, and specialized, technical knowledge. The impact on operations, though, promises to make the Division more collaborative between sections and with other agencies inside and out of the Justice community. Business processes will be more efficient and scalable as well. All this can be achieved without intruding on the organizational autonomy of individual sections.

Recommended Solutions

The issues presented form a formidable architectural challenge rooted in decades of non-compliance and patchwork attempts at maintenance. Fortunately, the trials facing the Criminal Division operate with some significant overlap, where fixing one challenge will ultimately bleed into addressing other concerns. Due to the highly interdependent complexity of implementation though, moving an element will likely impact dozens or more elements (Kotter 2012, 142). Service-Oriented Architecture circumvents these issues to a degree by offering "results in the short term while moving government toward the longer-term goal" (Wagner 2007). That said, SOA is not a magic bullet and will not solve the long-term issues facing the Division. Therefore, a transformation strategy is recommended in parallel to SOA.

Transformation Strategy

Because change cannot happen all at once, having a transfer plan is integral to success. The plan must establish benchmarks and measurements for business, data, applications, and technology in development of the target (Abbas, Fereydon, and Ali 2008, 2).

Address the Culture and Business Processes

The first step towards a vision of Enterprise Architecture solution, beyond the identifications already made, is to gain buy-in of the vision from leadership. Leaders who are willing to think in the long-term (decades or more), and are willing to make large amounts of change, will implement broad-based actions to empower workers to enact that change (Kotter 2012, 150). Additionally, a Guiding Coalition must be established to avoid hierarchical, or top-down approaches to solutions. The right team will consist of a mixture of those with positional

power, expertise, good reputations, and strong leadership skills (Kotter 2012, 59). The digital

transformation takes into account the whole ecosystem when "designing the digital future,"

and talent, working together, can help to define the change management of the vision, while

also influencing change to the culture (Ramesh 2016). Section chiefs, content professionals,

analysts, and information technology staff should especially be involved in this phase.

Once leadership is on board and a coalition is formed, and in order for definitive action

steps to take place, the organizational structure between information technology and the

Sections must remove barriers (Kotter 2012, 107). With this done, the definitive steps to act

and align the systems towards the architectural vision can begin to be applied.

Modernizing Legacy Systems

In order to save on expenses from maintaining legacy systems, as well as improve the

core processes of CRM, a modernization effort in accordance with the transition plan is

necessary (The White House Office of Management and Budget 2012, 42). The good news is,

Enterprise Architecture can be a "companion" for making the pivot towards a new system,

while keeping the old one running (Bente, Bombosch, and Langade 2012, 277). Modernization

can happen once the data that exists on the legacy system has found a new home. With the

new plan in place for data sharing and knowledge management, moving the data to a new or

temporarily new home is simply a technical challenge. Decisions on how it fits into the bigger

picture will have already been made. From that point, a new front-end for the data can be

moved to production, and the legacy system can be retired following testing and confirmation

that it is no longer needed. Change management tools at this stage will be helpful in tracking

changes and to watch overall progress (Bente, Bombosch, and Lengade 2012, 276).

Tracking the Budget

The fiscal goals for the Enterprise Architecture outcomes and vision implementation, can be achieved by quantifying improvements made through initiatives. The coalition will have to identify metrics by utilizing KPI's to measure the usefulness of an application or architecture. The following measurements should be made known to architects in order to study and make adjustments to initiatives (Bente, Bombosch, and Langade 2012, 69-70):

- Total cost of ownership of an application (TCO)

- Strategic fit of an application (SF)

- Value contribution of an application (VC)

- Fan-in and Fan-out of an application

By implementing these or similar metrics, quantification of savings can be measured as Enterprise Architecture solutions are enacted.

SOA in Parallel

While a transition plan is being put together and enacted, Service-Oriented Architecture with Web Services should act in parallel. This is because SOA has massive potential for enterprise-wide organizational transformation and cost savings without the need to solve immense structural challenges. SOA encourages Enterprise Architecture adoption because it has a "strong architectural focus, including governance, processes, modeling and tools" (Newcomer and Lomow 2004). The architecture recognizes "innumerable independent agencies" allowing information sharing to occur across Sections and agencies alike (Justice

Information Sharing 2004). This builds on the existing, but underutilized SOA already present at the Criminal Division, while providing an innovative, modern solution.

Core Business Processes

With SOA and Web Services, customers and IT have an independent system that allows for the easy creation of automated business process (Newcomer and Lomow 2004). Additionally, thanks to the ability to rapidly iterate, business processes and technology together can help to fine-tune the processes to be as easy to use and as efficient as possible.

Knowledge, Information, and Data, Enterprise Maturity

While the transformation plan acts to consolidate and collect data, an SOA can already utilize the disparate data sources and display them all in single or multiple locations across multiple web applications, with varying degrees of access and control. From an architect's view, this can even provide an easy way to organize the KID stuff for incremental moves towards a single database or storage solution, and the users and the Division can begin to see the benefits right away. In this way, a solution is provided by example – which is a powerful tool in gaining buy-in from holdouts in leadership as well.

This also tackles the issues of Enterprise Maturity – or at least the appearance of, by providing incentive and rapid application integration in order to give customers the automated business processes they need (Newcomer and Lomow 2004). It provides the Division with a strong modular system, with flexibility, stability, and high functionality-reuse. This is because it decouples functionality from technology and removes data from an end-user application and allows it to be accessible in the web (Bente, Bombosch, and Langade 2012, 68). The

technologies exist now for robust Web Services, and are increasingly powerful and operate across systems and platforms, allowing for a cohesive and modular front-end, even when the back-end is not capable of modern interoperability.

Security Throughout

Of course, as mentioned elsewhere, security will exist at all levels of implementation by helping to ensure solutions are safe and do not increase risk. This is mainly a passive role, but it is important to note their involvement at all levels of solution integration, SOA or otherwise.
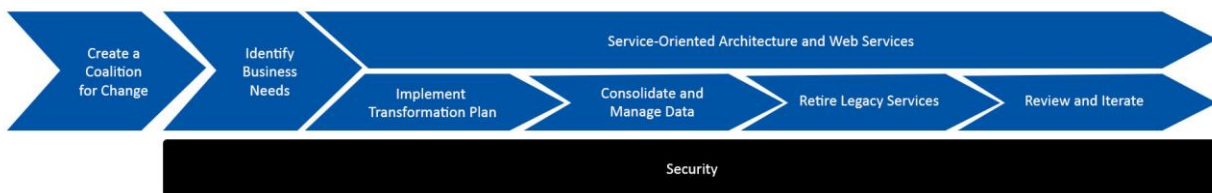
High-Level Roadmap Timeline

*Figure 3 - A High-Level Roadmap Timeline*

Conclusion

It is highly recommended to implement Service-Oriented Architecture with Web Services for all front-facing applications immediately. Enterprise-level application productivity can be achieved now with a web server and a browser and will encourage architecture improvements overall. In parallel to this, a transformation plan should be prepared and enacted as swiftly as possible to bring the rest of the organization into Federal Enterprise Architecture Framework compliance with the goal of achieving architectural maturity.

Appendices

The below image represents the catalog of data, systems, and actors currently existing within the Criminal Division. Currently, security (shaded area) encompasses all entities, but does not have influence over legacy systems. The data and solutions are all over the place, while other agencies have no access.
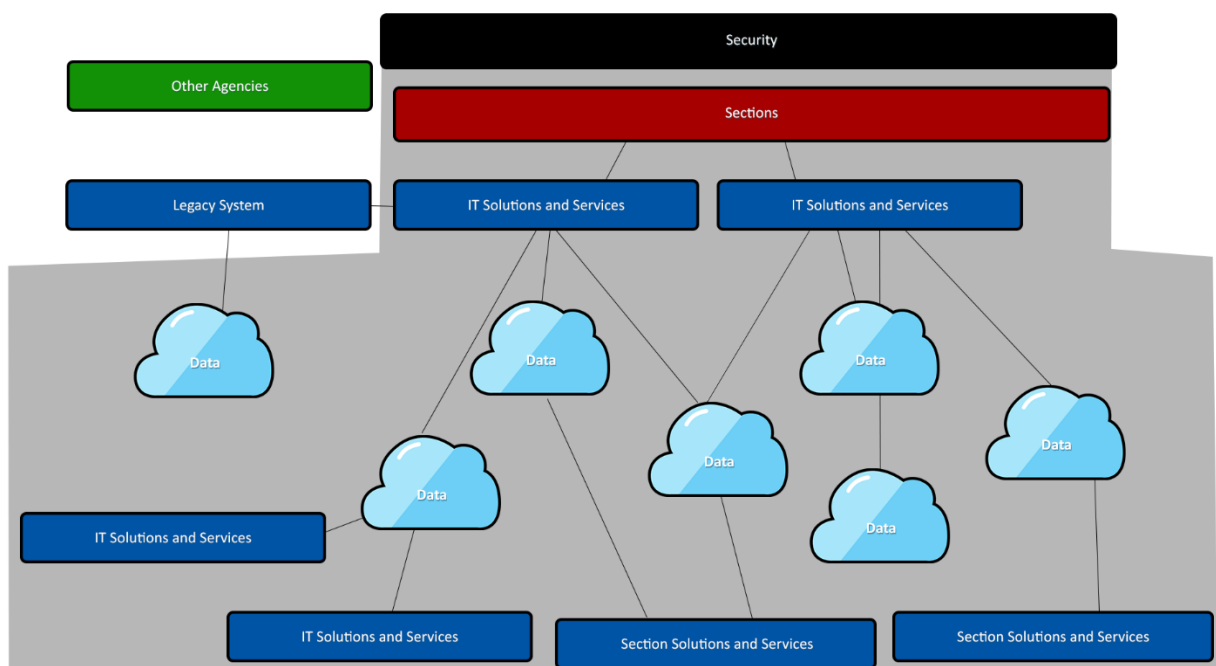
The next image is a representation of following the implementation of the Federal Enterprise Architecture Framework and Software-Oriented Architecture in conjunction with Web Services.
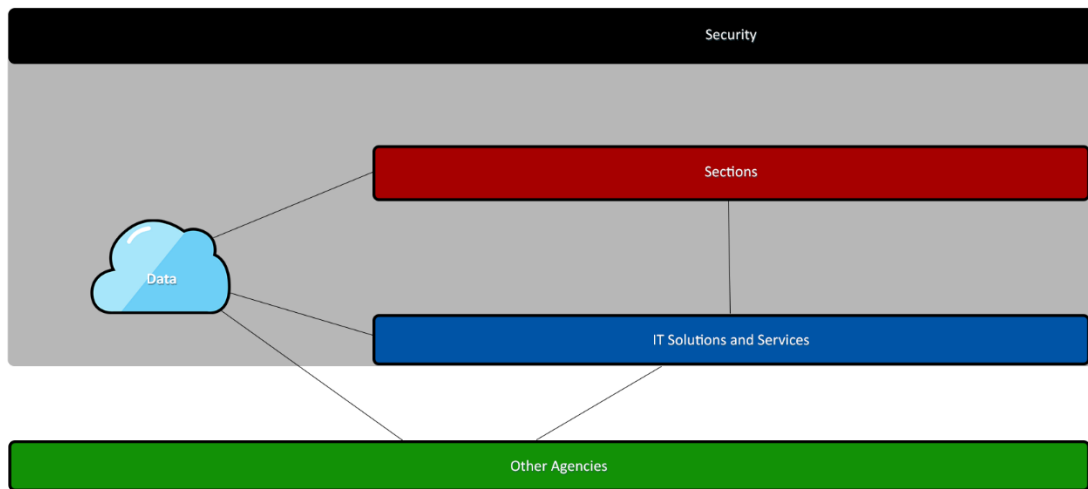
As can be seen, the architecture simplifies and brings all data into one place, providing and

sharing information across sections and agencies, while serving customers.

References

Abbas, Akkassi, Shams Fereydon, and Seyyedi Mir Ali. 2008. "Presenting A Method for

Benchmarking Application in the Enterprise Architecture Planning Process Based on

Federal Enterprise Architecture Framework." *2008 3rd International Conference on

Information and Communication Technologies: From Theory to Applications* (April 7-11,

2008): https://doi-org.du.idm.oclc.org/10.1109/ICTTA.2008.4529988.

Bernard, Scott A. *EA3, An Introduction to Enterprise Architecture.* 3rd Edition. Bloomington:

AuthorHouse, 2012.

Bente, Stefan, Uwe Bombosch, and Shailedra Longrade. *Collaborative Enterprise Architecture.*

Waltham: Elsevier, Inc., 2012.

Heffner, Randy. 2007. *The Forrester Wave: Standalone SOA and Web Services Management

Solutions, Q4 2007*, Forrester, October 22, 2007.

https://www.forrester.com/report/The+Forrester+Wave+Standalone+SOA+And+Web+S

ervices+Management+Solutions+Q4+2007/-/E-RES41971

Janssen, Marijn and Anthony M. Cresswell. 2005. "Enterprise Architecture Integration in E-

Government." *Proceedings of the 38th Hawaii International Conference on System

Sciences* (January 6, 2005). https://doi-org.du.idm.oclc.org/10.1109/HICSS.2005.243

Justice Information Sharing. 2004. *A Framework for Justice Information Sharing: Service-

Oriented Architecture (SOA).* The Global Infrastructure/Standards Working Group,

December 9, 2004. https://it.ojp.gov/documents/Service-OrientedArchitecture12-

04.pdf

Justice Information Sharing. 2005. *Global Justice Information Sharing Initiative: Exploring*

Service-Oriented Architecture Services for Justice Information Sharing. Global Justice

Information Sharing Initiative: United States Department of Justice, 2005.

https://it.ojp.gov/documents/SOAServices.pdf

Kotter, John P. 2012. *Leading Change.* Boston: Harvard Business Review Press, 2012.

Newcomer, Eric, and Greg Lomow. *Understanding SOA with Web Services: Introduction to SOA*

with Web Services. London: Pearson Education, Inc. 2005:

https://learning.oreilly.com/library/view/understanding-soa-

with/0321180860/ch01.html

Raj Ramesh. "A Blueprint for Digital Transformation." 2016. YouTube video, 6:23. Posted

February 4, 2016. https://youtu.be/zi0OaLMWYRA

Ross, Jeanne W., Weill, Peter, and David C. Robertson. 2006. *Enterprise Architecture as a*

Strategy. Boston: Harvard Business School Press, 2006.

US Department of Justice. 2017. "About the Criminal Division." Last Modified January 18, 2017.

https://www.justice.gov/criminal/about-criminal-division

US Department of Justice. 2016. *DOJ Order 0903 Information Technology Management*,

Approved by Lee J. Lofthus, Assistant Attorney General for Administration, May 5, 2016.

https://www.justice.gov/jmd/file/877186/download

US Department of Justice. 2016. *DOJ Order 0903.002 Information Technology Management*,

Approved by Lee J. Lofthus, Assistant Attorney General for Administration, May 5, 2016.

https://www.justice.gov/jmd/file/870291/download

US Department of Justice. 2019. *Department of Justice Information Technology Strategic Plan*

(FY 2019-2021), Joseph F. Klimavicz, Deputy Assistant Attorney General, Chief

Information Officer. nd. https://www.justice.gov/jmd/page/file/1141946/download

US Department of Justice. 2016. *Information Technology Governance Guide Version 7.0,* John

Raymond, Director IT Policy and Planning. September 16, 2016.

https://www.justice.gov/jmd/file/705831/download

US Department of Justice. 2019. "History." Last Modified July 25, 2019.

https://www.justice.gov/criminal/history

US Government Accountability Office. 2019. *Information Technology: Agencies Need to Develop*

Modernization Plans for Critical Legacy Systems, United States Government

Accountability Office Report to Congressional Requesters, June 11, 2019.

https://www.gao.gov/assets/700/699616.pdf

US Government Accountability Office. 2011. "Agencies need well-defined and implemented

enterprise architectures to avoid developing overlapping or duplicative information

technology systems." Last updated March 29, 2019.

https://www.gao.gov/duplication/action_tracker/Enterprise_Architectures_%282011-

14%29/action1

Wagner, G. Martin. 2007. "Why SOA matters." *Federal Computer Week* 21, no. 34 (October 15,

2007): 30, http://du.idm.oclc.org/login?Url=?url=https://search-proquest-

com.du.idm.oclc.org/docview/218865926?accountid=14608.

The White House Office of Management and Budget, *The Common Approach to Federal

Enterprise Architecture.* Obama White House, May 2, 2012.

https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/com

mon_approach_to_federal_ea.pdf