GITEC EMERGING TECHNOLOGY CONFRENCE

APRIL 28-30, 2019 | WESTIN ANNAPOLIS | ANNAPOLIS, MD

On behalf of the Advanced Technology Academic Research Center, I am proud to announce the release of a White Paper documenting the MITRE-ATARC Emerging Technology Collaboration Symposium held on April 29, 2019 in Annapolis, MD in conjunction with the GITEC Emerging Technology Conference.

I would like to take this opportunity to recognize the following session leads for their contributions:

MITRE Chair: John Griffith, Principal Artificial Intelligence Engineer, MITRE

Challenge Area 1: Security
Mark Bunn, Program Manager, DHS CISA
Kevin Cox, CDM Program Manager, DHS
Scott Davis, Deputy CISO, DOL
Vincent Sritapan, HSARPA Program Manager, DHS S&T
Rick Therrien, Director, Cybersecurity Architecture & Implementation, IRS
Ron Thompson, Director, Information Technology Division and CIO, USDA
Jeremy Wiltz, Assistant Director, IT Enterprise Services Division, FBI
James Aguirre, Director, Federal Civilian Sales, Check Point
Darren Death, VP of Information Security & CISO, ASRC Federal
Nick Murray, Account Executive, DHS, Splunk
Carten Cordell, Reporter, Washington Business Journal
Dr. Mari Spina, Principal Cyber Security Engineer, MITRE

Challenge Area 2: Digital Experience
Edward Dowgiallo, Principal Solutions Architect, DOT
Jacob Parcell, Director, Innovation Portfolio, Technology Transformation Service, GSA
Jim Tunnessen, CIO and Chief Digital Officer, Voice of America
Jory Heckman,Reporter, Federal News Network
Trevor Bostic,Sr., Computer Scientist, MITRE

Challenge Area 3: IT Modernization
Ben Bergersen, CIO, USTDA
Denise Hill, Senior Technical Advisor, DOE
Keith Nakasone, Deputy Assistant Commissioner, GSA
Harrison Smith, Acting Senior Procurement Executive, Treasury Department
Nicole Johnson, Managing Editor, GovLoop
Mano Malayanur, Principal Infrastructure Engineering, MITRE

Below is a list of government, academic and industry members who participated in these dialogue sessions:

Challenge Area 1: Security
Larry Acker, DSS; Robert Aitken, HHS; Michael Brotzman, DOD; Rich Burke, USMC, Taylor Cato, Carahsoft; Adam Cowdery, DOS; David DeVries, Dataguise; Paul Hill, FRTIB; Russ Holmes, Merlin; Tony Hudnell, EPA; Brandi Mix, DOT; Jason Ng, DOS; Chuba Oraka, University of the Potomac; Paul Sechser, Accellion; Barbara Stance, FAA

Challenge Area 2: Digital Experience
Daniel Bier, DOE; Marlene Chandler, DOS; Richard Eng, MITRE; Joel Fasanya, HHS; John Hsu, US Courts; James McGrath, DOT; Kelly Miller, Aerospace; Andrew Osborn, Zimperium; Ceresh Perry, US Army Corps of Engineers; Gary Reams, DOJ; Simoon Shiferaw, VA; David Smalley, Altair; David Vigna, DOD

Challenge Area 3: IT Modernization
Margeaux Akazawa, HHS; Gil Alterovitz, VA; Adam Chiou, DOD; Basil Coutifaris, IBM; Francis Campion, MITRE; Refayat Haque, HHS; Timothy Luc, MITRE; Wynn Meyer, NIH; Larry Nadel, NIST; Danny Nsouli, MITRE; Faith Ryan, Government CIO; Simon Szykman, Attain; Audrey Winston, MITRE; Yining Xie, NIH; Yuan Yao, GSA

Thank you to everyone who contributed to the MITRE-ATARC Emerging Technology Collaboration Symposium. Without your knowledge and insight, this White Paper would not be possible.

Sincerely,

Tom Suder
Founder, Advanced Technology Academic Research Center (ATARC)

FEDERAL SUMMITS

APRIL 2019
GITEC EMERGING TECHNOLOGY CONFERENCE REPORT*

February 17, 2020

John Griffith, Trevor Bostic, Mano Malayanur,
Mari Spina, Justin F. Brunelle
The MITRE Corporation

Tom Suder
The Advanced Technology Academic Research Center

*APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. CASE NUMBER 19-02491-4.

Contents

1 ABSTRACT

The GITEC Emerging Technology Summit was held on April 29, 2019. This was the first summit since the Government Information Technology Executive Council (GITEC) merged with the Advanced Technology Academic Research Center (ATARC). The summit included three MITRE-ATARC Collaboration Sessions. These sessions allowed industry, academic, government, and MITRE representatives the opportunity to collaborate and discuss challenges the government faces in adopting and utilizing emerging technologies. The goal of these sessions was to create a forum to exchange ideas and develop recommendations to further the adoption and advancement of emerging technologies and associated best practices within the government.

Participants representing government, industry, and academia addressed three challenge areas in the federal emerging technologies domains: *Security*, *Digital Experience*, and *IT Modernization*. Within those topics areas, several sub-topics were investigated by different groups. This added some unanticipated complexity and challenges (e.g., the leader for each room had to take notes from multiple, simultaneous conversations). This reduced the overall depth and continuity of the notes on each topic.

This white paper summarizes the discussions from the collaboration sessions and presents recommendations for government, academia, industry, and federal funded research and development centers while identifying intersecting points among challenge areas. The sessions identified several actionable recommendations for the government, academia, and industry:

- get a champion in senior leadership to shift culture and alleviate policy barriers
- invest in data to train automation solutions
- invest in artificial intelligence to reduce data overload challenges
- invest in staff, focusing on reskilling and upskilling of the existing workforce

2 INTRODUCTION

During the GITEC (Government Information Technology Executive Council) Emerging Technology conference, held on April 29, 2018, three MITRE-ATARC (Advanced Technology Academic Research Center) Collaboration Sessions gave representatives of industry, academia, government, and MITRE the opportunity to discuss challenges the government faces in adopting and utilizing emerging technologies. Experts who would not otherwise meet or interact used these sessions to identify challenges, best practices, recommendations, success stories, and requirements to advance the state of emerging technologies use and research in the government. Participants ranged from the CTO, CIO, and other executive levels from industry and government to practitioners from government, industry, and federally funded research and development centers (FFRDCs) to researchers, students, and professors from academia.

The MITRE Corporation is a not-for-profit company that operates multiple FFRDCs [12]. ATARC is a non-profit organization that leverages academia to bridge between government and corporate participation in technology. This was the first GITEC conference since the ATARC-GITEC merger [10]. MITRE works in partnership with ATARC to host the collaboration session portion of the ATARC Federal Technology Summit Series of which the GITEC conference is now a part. The invited collaboration session participants across government, industry, and academia worked together to address challenge areas in various emerging technology domains, as well as identify courses of action to be taken to enable government and industry collaboration with academic institutions. Academic participants used the discussions as a way to help guide research efforts, curriculum development, and to help produce graduates ready to join the work force and advance the state of their research and work in the government.

This white paper is a summary of the results of the collaboration sessions and identifies suggestions and recommendations for government, industry, and academia while identifying cross-cutting issues among the challenge areas.

3 COLLABORATION SESSION OVERVIEW

Each of the three MITRE-ATARC collaboration sessions consisted of a focused and moderated discussion of current problems, gaps in work programs, potential solutions, and ways forward regarding a specific challenge area. At this conference, sessions addressed the following broad topics:

- Security
- Digital Experience
- IT Modernization

This section outlines the goals, themes, and findings of each of the collaboration sessions.

3.1 Security

The *Security* collaboration session was marked by a panel lineup of government and industry leaders in IT security and over 70 collaboration session participants. The topics covered the gamut from operations and governance to specific threats and technologies.

3.1.1 Session Goals

This session set goals to discuss challenges and solutions around the following topic areas:

- Security Operations/Situational Awareness for Agency Data in the Cloud
- Cryptographic/Key Management for Managing Access to Agency Data in the Cloud
- Mobile Threat Management
- Incident Detection and Response Optimization Across All Platforms and Data
- Channels Analytics and Business Intelligence for CDM-Reported Data
- Ongoing Assessment and Authorization to Transform Traditional Cybersecurity Compliance Reporting
- Managing the Lifecycle of Identities and Access
- Optimal Data Protection Mechanisms for High-Value Data

3.1.2 Session Summary

The collaboration session was initiated by a panel discussion. Panelists included visionary cyber security leaders providing coverage of network defense, continuous diagnostics and mitigation (CDM), cyber analytics, and enterprise security systems and architectures. Industry executives rounded out the panel to provide capability and technology perspectives.

The panel discussions addressed the state of The Department of Homeland Security's CDM initiative[1], which is in phase 2 of its instrumentation investment plan to "know who is on the network". It was noted that organizations should re-evaluate their High Value Assets (HVAs) and to possibly reconsider their systems and data Risk Management Framework (RMF) categorizations; not all systems need to be categorized at the "high" baseline, which can require larger investment. Enterprise Security Operations Center (SOC) standup is a currently a focus of government organizations and consolidation of the various operating centers and the multitude of support tools is driving planning. Current Trusted Internet Connection (TIC) pilots in process are driving the evolution of the TIC 3.0 pending policy guidance[2] [4].

For the open collaboration segment of the Security session, participants were divided up into the following eight topics areas each with a panelist as lead facilitator:

- Security Operations/Situational Awareness for Agency Data in the Cloud
- Cryptographic/Key management for Managing Access to Agency Data in the Cloud
- Mobile Threat Management
- Incident Detection and Response Optimization Across all Platforms and Channels
- Data Analytics and Business Intelligence for CDM-Reported Data
- Optimal Data Protection Mechanisms for High Value Data
- Managing the Lifecycle od Identities and Access

Each table practically filled at 8 participants. With respect to the assigned topic, each table of participants was asked to describe their challenges, lessons learned, and recommendations.

3.1.3 Topics

This section provides summaries of the discussions on each of the topic areas. Each summary addresses the challenges, lessons learned, and recommendation from the focus group.

3.1.3.1 Security Operations/Situational Awareness for Agency Data in the Cloud

[1] `https://www.cisa.gov/cdm`
[2] `https://cloud.cio.gov/strategy/`

Challenges Government organizations continue to wrestle with the impact of cloud technologies on cyber operations and situational awareness. Each cloud service brings its own set of security logs and maintenance activities. The shared responsibility model not only requires an understanding and agreements between cloud providers and cloud consumers but also between cyber operations and systems operations and maintenance organizations. Of importance to the focus group were the following associated challenges:

- Difficulty understanding service provider SLAs and shared responsibilities
- Growing pains associated with adopting the new business model based upon consumption as opposed to sustainment
- Estimating migration costs during or due to technological change
- Applying policies to evolving IT technologies that were intended for application to legacy systems

Lessons learned History continues to illustrate the need for advanced and evolving skill sets when business paradigms change. In some ways, the cloud has disrupted business as usual and the need to retool personnel skill sets is ever apparent. Key lessons learned expressed by the focus group include the following:

- Proper system scoping is important
- Driving cultural buy-in is key to successful adoption of improved technologies
- Cybersecurity mandates are easy to implement through compliance mechanisms
- Build security into the DevOps pipeline; this will improve compliance and assurance levels
- The learning curve may be steeper than anticipated by the adopting organization

Recommendations For those setting out to successfully adopt cloud technologies, the focus group offered these words of advice:

- Start small; share and collaborate with industry and sister organizations
- Validate investment and design plans with the Authorizing Official (AO) and Service Providers as early as possible
- Automate as much as possible

3.1.3.2 Cryptographic and Key Management for Managing Access to Agency Data in the Cloud

Challenges Protecting data in the cloud has become a complex endeavor. Cloud consumers continue are sensitive to the possibilities of losing control over their data assets, however rare or common this may be. Many consumers simply do not know where to start the process of protecting cloud data. Accordingly, the focus group expressed the following challenges:

- Data protection standards can be difficult to understand
- Executive drive to deployment tends to result in incompletely protected systems
- There are never enough resources

Lessons learned As with all new technologies, the learning curve can be steep, but what happens when adoption is slow and lessons are few and far between? This is when extrapolation from peer groups becomes very important. Accordingly, the focus group expressed the following realizations:

- This is a new field for many organizations venturing outside their typical perimeters; lessons are not abundant
- It is essential to build in resilience to cyber failures
- Cultivate understanding of risks of data in the cloud

Recommendations Finally, for those looking to protect data assets and cover the risks of data loss, the focus group made the following recommendations:

- Implement enterprise key management solutions
- Get senior executive sponsorship early in the modernization process
- Push for federal mandates to be sure data security happens as a function of compliance

3.1.3.3 Mobile Threat Management

Challenges Mobility is changing business for good. Wireless is enabling improved mobility and connectivity, but as the workers become increasingly more mobile and mobile system technologies evolve, the cyber threat landscape grows. Unfortunately, understanding the mobile threat landscape is not yet a priority. The focus group specifically cited the following challenges:

- There is no real mandate for mobile threat management (MTM) and the definition and capabilities vary across service providers
- There are no security controls in the National Institute of Standards and Technology (NIST) standard 800-53 [8] for bring your own device (BYOD) systems
- CDM solutions for mobile devices are neither well defined nor supported in the marketplace

Lessons learned With challenges inevitably come lessons learned. The following lessons point to the need for balance between policy and leadership:

- NIST's National Cybersecurity Center of Excellence (NCCoE) Lab[3] derived guidance is valuable
- Ensure cloud based MTM is FISMA [3] compliant
- Leadership should understand the challenges in cultivating buy-in, provisioning systems, and security mobile devices

Recommendations This focus group was of the opinion that government leadership was necessary to make a real impact. Accordingly, they offered the following advice:

- Create a government mandate for MTM
- Adequately resource MTM programs
- Push for NIST 800-53rev 4 MTM based controls [8]
- Update FISMA requirements to include metrics for mobile asset management

3.1.3.4 Incident Detection and Response Optimization Across all Platforms and Channels

[3] `https://www.nccoe.nist.gov/`

Challenges The challenges expressed in this area are reminiscent of those that recur as industry struggles with the shared responsibility model that the cloud ushers in.

- There exists uncertainty regarding who is in charge of incident response when responsibilities are shared between cyber defenders and system developers complicates and delays response and mitigation.
- In some environments, government users feel blind to cyber incident detection.
- Staffing and resourcing cyber defense with appropriately skilled workforceremains a problem; too few people are available to do the job.

Lessons learned As the story goes, more information is always better than too little. But too much can also be a burden. As cloud migration hastens, organizations are finding that the claimed answer to cyber compliance in the cloud all too often creates a deluge of data that the organization is simply unable to handle. As a result, cloud consumers continue wrestle with the reliable resourcing of the following practices:

- Government agencies own a lot more assets than are used but not everything needs visibility
- Use threat intelligence to move mitigation to earlier in the detection and response
- Alert information is abundant, yet high fidelity alerts are difficult to attain

Recommendations In this area, strides have been made to cope with the challenges presented by cloud adoption and the complexities of the shared responsibility model. For those in the cloud now and looking to move to production, the focus group offered the following suggestions:

- Use delegation of authorities to drive responsibilities; Standard Operating Procedures (SOPs) and playbooks will help to solve the shared responsibility issues and standardize methods
- Invest in Security Orchestration Automation and Response (SOAR) platforms

3.1.3.5 Data Analytics and Business Intelligence for CDM-Reported Data

Challenges This topic included discussions of data overload; with large volume streaming data comes the need to establish data handling techniques that optimize analytics. Accordingly, the focus group made the following observations with respect to the challenges:

- We are awash with data and building rule sets against the volume of data available is extremely laborious
- CDM dashboards can be misleading
- Adversaries are evolving, yet the available data necessary for threat detection is not evolving to match adversary tactics

Lessons learned It was noted that CDM data and cyber event data should not be considered in isolation of each other and the focus group made the following observations:

- CDM dashboard can be too siloed
- Effective NOC/SOC collaboration is key developing signatures and analytic rule sets

Recommendations For the practitioners working to make cloud migration effective now, the focus group made the following suggestions:

- Invest in machine learning (ML) and artificial intelligence (AI) for threat detection
- Agencies should align cyber defenders with CDM systems
- Create a roadmap for cyber defense investments
- Build automation into threat mitigation solutions

3.1.3.6 Optimal Data Protection Mechanisms for High-Value Data

Challenges When protecting data assets, the following challenges are likely encountered:

- Determining the location of threats on the network given the volume of data is difficult
- Detecting and categorizing general network attacks including Man-in-the-Middle (MiTM) is difficult
- Distributed denial of service attacks and malicious attachments are common
- Credential attacks can be difficult to detect

Lessons learned The realization that cyber attacks are a prominent that is reinforced by the following observations:

- Compromise is a question of "when" not "if"
- There are no non-participants; all users can become a vehicle for attack

Recommendations For those whose job depends on keep data safe, the focus group made the following recommendations:

- Implement strong authentication solutions
- Use encryption everywhere
- Apply Data Loss Prevention (DLP) systems
- Use intrusion prevention and detection systems at network aggregation points
- Consider Zero-Trust technology options for access control [2]

3.1.3.7 Managing the Lifecycle of Identities and Access

Challenges Identity credential and access management (ICAM) continues to grow in importance as traditional on-premise private network infrastructure gives way to the cloud-based solutions using the internet. But the challenges of doing ICAM correctly have not become any easier. Accordingly, the focus group express the following challenges:

- All avenues of access are available for attack
- Device identity solutions are difficult to implement
- Personal Identity Verification[4] (PIV) authentication is insufficient to protect systems; PIV revocation is not tied to human resources and administration systems

[4] A Personal Identity Verification (PIV) credential is a US Federal governmentwide credential used to access Federally controlled facilities and information systems at the appropriate security level.`https://piv.idmanagement.gov/`

Lessons learned ICAM solutions are run by humans, meaning the solution implementation may be flawed. As a result, the focus group made the following lesson observations:

- PIV is not practical for use on devices without reader systems
- The user lifecycle needs to be managed to include HR and administration interfaces
- Do not put Access Lifecycle management (ALM) systems on the network front line boundaries; protect them with layered defenses

Recommendations Finally, for those attempting to implement ICAM solutions right today, the focus group suggested the following actions:

- Integrate HR and Administration operations with ALM solutions for more complete lifecycle management that is aligned to user management
- Train staff adequately; there are too many possible gaps in today's ALM approaches

3.1.4 Session Recommendations

It is clear from these discussions that government and industry continue to wrestle with recurring themes in cybersecurity. Data security, access and credential management, cyber defense operations, and instrumentation for compliance continue to provide rich soil for the innovative commercial vendor seeking to ease the load on their government counterpart.

Most of all, collaborations like these (e.g., informal meetings, information sharing systems, and the simple working lunch between coworkers) continues to improve skills and elevate awareness of cybersecurity trends. Government-Industry partnerships are recommended to foster "try it before you buy it" opportunities. Such opportunities and the inherent collaborations operate to enhance product effectiveness, improve the knowledge and skills base and bring the market sector closer to impenetrable defense.

Several recommendations resonated throughout this discussion group that could apply to almost any cybersecurity solution.

- Start small and scale up
- Create a roadmap for your cyber defense investments
- Validate investment and design plans with the AO and Service Providers as early as possible

- Get senior executive sponsorship early in the modernization process

These notions apply broadly to a vast array of cybersecurity concerns so much so, one might consider them heuristics of the practice.

However, that is not to say that technology specific recommendations did not also surface. Technology specific recommendation included the following:

- Integrate HR and Administration operations with ALM solutions for more complete lifecycle management that is aligned to user management
- Implement strong authentication solutions
- Use encryption everywhere
- Apply DLP systems
- Use intrusion prevention and detection systems at network aggregation points
- Invest in ML and AI
- Align cyber defenders with CDM systems
- Create a government mandate for MTM
- Push for NIST 800-53rev 4 MTM based controls
- Update FISMA requirements to include metrics for mobile asset management

These are indicators that implementation continues to create unforeseen costs. These specific areas could, therefore, be envisioned as fruitful soil for innovation, Government-Industry collaborations, and topics we might consider in discussions with leadership when asked, “Where do you think we can improve?” Further recommendations are included in the ATARC-MITRE 2019 CISO Summit paper [9].

3.2 Digital Experience

The session on digital experience gathered a group of experts to highlight the current state of the art technologies currently affecting user experience and to offer advice on what the way forward may look like. The session began with a panel of experts sharing their insights and then broke up into groups formed around particular subject areas. During the panel and groups, participants discussed the potential technologies that could be used to improve the

user digital experience, and what pitfalls for those technologies may be. Finally, participants discussed what changes the believed would be needed and where those changes would need to be implemented for maximum effect.

3.2.1 Session Goals

This session set goals to discuss challenges and solutions around the following topic areas:

- Modernizing user digital experience within the government
- Advise the government on policy decisions relating to creating a better digital experience
- Examine possible benefits of AI in the user experience workflow
- Determine strategies for quickly and efficiently implementing a modern digital experience

3.2.2 Session Challenges

The group identified the following overall challenges with digital experience in government environments:

- Legacy systems resistance to update/change
- Updating to new and possibly unfamiliar digital experience design patterns
- Customizing the user experience by user without invasion of privacy
- Inflexible policy unable to cope with modern paradigms
- Difficulty changing workforce culture
- Adopting and implementing technology

3.2.3 Session Summary

The digital experience session began with a panel lead by a moderator. Afterwards, the panel split up into groups with the session participants and lead discussions on their relevant expertise. The first group primarily focused on the modernization of customer experience in the ever-evolving world of digital media. The second group concentrated on AI, with

particular interest on possible future workflows for internal users looking to integrate AI into their own solutions. This section begins at a high level by discussing several of the large topics broached during the panel session by both panelists and participants.

The panel began by acknowledging that the main goal is for the government to be able to provide a digital experience equal to or better than the digital experience offered by many private companies. Before delivering such an experience, the first necessity is to better understand the end user for each process. Generally, this means understanding problems faced by citizens and employees, and potentially many subsets of these groups such as military members, contractors, disabled users, etc. Introduction of more advanced CRM tools was one suggestion given as a potential area for improvement. These tools would work to better understand the stories behind different users, measure user engagement, collect data on their experiences (e.g., difficulties completing a key workflow), or for collecting user data for use in predictive analytics that could help tailor more personal experiences.

Next, the panel discussed possible solutions for reaching a better digital experience efficiently and effectively. The common opinion among session participants was that the further automation and abstraction of daily processes would allow for meaningful work that positively impacted the user. Technology solutions suggested included Robotic Process Automation (RPA) and its AI enhanced counterpart, Intelligent Process Automation (IPA). The goal is that these technologies could be leveraged as cheap automation for standard activities or as routines meant to augment a given user. However, there are worries that these processes may be fragile over the long term and could cause a decrease in centralization and standardization. A counter-proposal offered was to further integrate APIs into necessary systems, incurring higher startup cost but retaining better control and structure over the system(s). Finally, there was the concession that RPA will need further maturation and a designed set of best practices before we see a large return on investment in the technology.

As a final topic, the panel and participants discussed what they believed to be the government's biggest challenges preventing a modern digital experience. Among the challenges given were the difficulty in changing the culture of the workforce, balancing security and usability, and enabling faster transformation with respect to technology. Culture change is currently being experienced by many organizations, and the current hope is that policies put forth to empower and re-skill the worker will naturally lead to a shifting work culture. The government's challenge of balancing security and usability is the risk tradeoff between providing an easy and enjoyable experience versus having high security requirements that may cause more work for the user. This challenge is seen as requiring the adoption of a risk-based model able to weigh the tradeoffs appropriately for each use case. Lastly, to hasten

our technology transformation we must have flexible policies built towards adopting new technologies as they become available. Modern day examples include the push towards mobile availability of content or the custom tailoring of content per person.

3.2.4 Topics

As the panel session drew to a close the panel leaders split up with the participants into two groups. The first group discussed customer experience within the realm of digital experience. The second group focused on AI and how it should be properly implemented. Each group discussed the possibilities offered by the adoption of their respective technology and standards. They then went on to examine the barriers and challenges that would be faced in creating, implementing, and standardizing the technologies. At the end of their sessions, they offered advice on how best drive change at multiple levels of government to achieve a concerted movement towards a better experience.

3.2.4.1 Customer Experience The customer experience group discussed the topic of customer experience modernization within digital media. Specifically, they focused on the factors that could drive the governmental change at lower (i.e., technical) and higher (i.e., policy) levels. They ended by offering insight on how to measure progress and success as we begin to execute this process. As mentioned earlier, the main belief of this group is that the government should have user experiences equal or exceeding that provided by their private counterparts.

For technical goals, the group recognized that modern design of forms and mobile first sites must be emphasized. Additionally, they found the ability to share common design patterns and to detach backend legacy systems from their front-end to be of great value. The group found the current conventions for forms antiquated and discussed a movement to a "Turbo-Tax" style of interactive forms. In this paradigm, the user is guided by varying questions and suggestions based upon their personal information. This greatly increases the customer experience, especially in the case of complex forms.

In the same vein as streamlining forms, a mobile first design is meant to allow users to access important functions quickly and with few interactions. This complements a current cultural shift whereby many users now prefer to access these services through their mobile devices instead of a traditional computer.

To further increase efficiency, the design and use of common "building blocks" was recommended. One participant discussed the U.S. Web Design System 2.0[5]. This system

[5] `https://designsystem.digital.gov/`

demonstrates many common use cases and allows viewers to immediately extract and use the code as the "building blocks" for their applications. Further work and research may be necessary to encompass the various frameworks seen throughout the field but should follow the general approach provided.

As the final technical goal, the participants noted that there would be a great deal of value in government achieving the capability of disconnecting back-end operations from the front end. This would significantly decrease the risk in modifying and updating the front end as it would minimize the downtime of the application. Moreover, it extends the lifecycle of the backend, reducing the cost of maintaining the application overall.

On the policy side, participants believed that improvements in customer experience benefit from a top down approach. With executive buy-in, contracts could be written emphasizing customer experience using terms such as usability, accessibility, and inclusive, possibly even requiring successful use of GSA accessibility tools for measurement. In addition, they looked for leadership in re-skilling the workforce, which they believe will bring about gradual change in work culture. Finally, if all else failed, they thought laws such as Section 508 [5] might ignite action.

To measure the success of these actions, the group advised government creation and monitoring of Key Performance Indicators (KPIs), especially including those related to customer feedback and data collection from use. The customer feedback will most likely be generated via surveys. Data collection from use on the other hand may have some interesting and creative solutions to be explored. Ideas such as analysis on user progress on workflow before quitting, user difficulty finding key workflow, and others may give great insight on the actual user experience instead of just the reported user experience.

3.2.4.2 Artificial Intelligence in Customer Experience Just as the customer experience had a main question to answer, so too did the group on AI: What role does the government play in helping standardize and regulate how AI is used in supporting the digital experience within government functions? As they discussed this question, they breached the topics of AI privacy, its domain of use, and centralizing AI solutions to enable wider spread use.

In the discussion on AI privacy, the main worries were for what personal data owned by the government may be accessed and what its uses should be. The main problem noted was re-identification, a process whereby a user's identity can be deduced when data from one or more anonymous systems are collected and matched together. Possible solutions were the creation of standards on managing AI related projects and how the data was retrieved, cleaned, and used.

Next, they delved into possible use cases where AI may help and discussed the possible barriers for each scenario. A common opinion was that it was worth additional investment investigating low-key government process that have not received consideration but may be automatable. The thought process was that AI may be simple to implement in some unconsidered cases, and implementation could offer an opportunity to receive an immediate return on investment. As before, there were considerations on AI privacy, but also concerns over AI transparency. Depending on the context, black-box methods such as deep-learning may be ill-suited or even destructive for government purposes. The group held that consideration for more transparent approaches should be required in high risk scenarios so the AI logic can be checked by humans. As an example, consider a system helping judges decide verdicts.

Lastly, the participants discussed potential strategies for centralizing AI that would both help standardize procedures and allow for more widespread use by non-experts. A first step mentioned was the creation of inter-agency or multi-agency advisory committees to oversee the efforts. Then, on a technical level, they would look to have a common repository of data and pre-trained models for users to draw from. The data would ideally have gone through appropriate standardized approval and cleaning process as listed above before use, ensuring safe practices for potential users. Furthermore, the use of pre-trained models augmented by area-specific data could allow for a shallower learning curve for non-experts to apply AI to their field. To achieve these goals, it was also advised that the government retain its technical talent as best as possible.

3.2.5 Session Recommendations

Several recommendations came out of this session.

- Survey current data practices both internally and externally.
  - Creating standards/best practices for data retrieval, cleaning, and usage. These standards/best practices are meant to help practitioners on a technical level, while also keeping them mindful of potential data privacy and sensitivity issues such as re-identification.
  - Determine data sets and/or AI approaches commonly used that would benefit from widespread availability. The goal is to give practitioners the option/ability to build off of previous work.
- Implement CRM systems capable of storing customer data, feedback, and data within context of experience. The goal is to enable design for the modern use case, which may

necessitate practices such as chatbots, mobile first, or interactive forms.

- Shift culture through an emphasis on re-skilling workforce on modern technologies and change of common language. The belief held by the participants was that re-skilling and change of language, such as that found in contracts, would ultimately shift culture over time.
- Create organizational effort for maintaining "organizational memory" to better retain technical and non-technical experience.
- Focus on detecting staff that could benefit from process automation of usual "busy work" tasks and repurposed for meaningful work.

3.3 IT Modernization

The session on IT Modernization brought together experts from government, industry, and academia to discuss issues around IT Modernization affecting the government.

3.3.1 Session Goals

The topics selected for IT Modernization track included the five centers of excellence established by GSA[6]: Cloud Adoption, Contact Center, Customer Experience, Data and Analytics, and Infrastructure Optimization. Additional topics such as Culture were also included. Of these, the assembled participants selected the following three topics for breakout sessions:

- Cloud Adoption
- Culture
- Data and Analytics

3.3.2 Session Summary

Each session was moderated by a government lead and included representation from government, industry, and academia. The participants deliberated their topic areas and identified challenges and opportunities, best practices, and recommendations in their topics, summarized in this section.

[6] `https://coe.gsa.gov/`

3.3.3 Topics

The topics of Cloud Adoption, Culture, and Data and Analytics are presented below.

3.3.3.1 Cloud Adoption This section describes the challenges and opportunities, best practices, and lessons learned, and recommendations discussed by the Cloud Adoption breakout session.

Challenges and Opportunities Challenges to cloud adoption are often those of any significant initiative pursued by government agencies. Often prevalent culture comes in the way of significant changes. An example is an instance of requiring cloud vendors to conform to an agency's Technology Reference patterns, architectures, and third-party software versions, rather than modify the agency's guidelines to adopt to cloud environments. Lack of expertise also often is a challenge with cloud computing. These themes were discussed in the session.

External factors are often catalysts to cloud adoption (e.g., aging data centers which require considerable investments) which makes cloud computing often attractive. The Data Center Optimization Initiative[7] requires data centers to be closed; this often opens up opportunities for cloud adoption. The session participants identified several challenges and opportunities pertaining to cloud adoption.

- User buy-in and cultural shift: Due to a multitude of reasons such as potential lack of control, buy-in and cultural shift required for cloud adoption remain a challenge.
- Is the government really hiring for the cloud? Lack of sufficient workforce skilled in the use of cloud services remains a major challenge.
- Need new and modern thinking: As is true of disruptive technologies, the use of cloud services require new thinking. An example includes the use of managed services and "serverless" computing, instead of replicating an on-premises infrastructure in the cloud with virtual machines and load balancers.
- Playbooks are acting more like tutorials: Lack of expertise has implied that playbooks take on a different role.
- Mandate of shutting down data centers may be an opportunity: Mandates such as the Data Center Optimization Initiative require a reduction in the number of data centers. Cloud environments may provide a convenient alternative.

[7] `https://datacenters.cio.gov`

- Ageing data centers may be an opportunity: Likewise, aging data centers and the costs associated in their maintenance may propel the use of cloud environments instead.
- Continued use of continuing resolutions restricts the vision and use of long-term budget: Uncertainties regarding future budgets hamper visionary initiatives such as cloud.
- Not making a decision versus making the wrong decision: Fear of making the wrong decision hinders cloud adoption.
- Changing the legacy thinking culture: Encouraging a movement away from a "not invented here" mentality.

Best Practices and Lessons Learned Successful initiatives often require leadership, communication, organizational readiness, and funding; cloud adoption is no exception. Such initiatives often have support from senior levels in the agency. Communication and organizational change requires listening to stakeholders and addressing their concerns. Securing the requisite funding, based on business case analyses, cost benefit analyses, and total cost of ownership analyses, is a key ingredient for successful cloud adoptions.

The session discussed and developed several best practices and lessons learned.

- Create a sense of urgency: This helps rally support for the initiative.
- Need a strong implementer to help with hurdles: Given the scope and size involved in cloud adoption initiatives, hurdles will be inevitable, and strong leadership is required to overcome them.
- Identifying SaaS compromises up front rather than customization; By its nature, cloud services, particularly SaaS, require modifications in business processes.
- Budget cuts are an opportunity for cloud adoption: Well implemented cloud solutions have the potential for cost savings.
- CIOs and CFOs need to be on the same page: Federal Information Technology Acquisition Reform Act (FITARA) [1] enhances the CIO authorities and helps achieve this best practice.
- Needs to come from the secretary level: Leadership support, at the highest levels of the agency, often removes obstacles.

- Capability roadmap directly tied to funding: Funding brings with it the needed resources and accountability to major initiatives such as cloud adoption.
- Understand the root of people's concerns (e.g. security) and addressing them – don't just state the facts.
- Types of moves to the cloud include Small (e.g., email), Medium (e.g., CRM, SharePoint), or Large (e.g., mission critical applications)

Recommendations The themes of leadership and communication were prominent in the group's recommendation. Working groups, both within and across agencies, are helpful in learning lessons. Lastly, in cloud adoptions, careful attention to requirements is key; requirements that differentiate between what the cloud service provider (CSP) is responsible for versus an integrator or a broker, who uses the CSP services to build systems to meet agency requirements.

The group derived the following recommendations.

- Create working groups across agencies to make sure everyone buys-in and so that you create champions
- Include mission folks and security folks in working groups with IT; consider drafts for public comments for crowd-sourcing
- Change needs to come from the top
- Transition adoption needs to get more attention in Requests for Proposals (RFPs)
- Let the marketplace decide the winner (i.e., CSP) but using very clear requirements and desired outcomes

3.3.3.2 Culture In the article "5 Myths of Change Management for IT Modernization"[8], the authors note the importance of an organization's culture and the ability to absorb change. Success in IT modernization requires an organization to take proactive steps in overcoming challenges posed by the prevailing organizational culture in an agency. The breakout session on culture discussed the following challenges, opportunities, best practices, lessons learned, and recommendations related to culture in IT modernization.

[8] https://www.boozallen.com/s/insight/blog/5-myths-of-change-management-for-it-modernization.htm

Challenges In a Working Paper at the Massachusetts Institute of Technology titled "Organizational Challenges in Cloud Adoption and Enablers of Cloud Transition Program"[7], the author Sneha Rajendran notes:

> The implementation of cloud in an organization however brings in changes in the IT and business operations. These shifts pose challenges related to governance, security, dependency and changes in the roles and responsibilities of employees working in the business and IT functions of the organization.

IT modernization, more broadly, often effects similar changes and poses similar challenges to the organization.

The working session identified several challenges related to culture.

- Not sharing information within agency/subcomponents and/or with other agencies: lack of adequate communication is a familiar issue in transformation initiatives.
- People often a "feel" like they have to hold the work "proprietary" and do want to share due to personality or sense of ownership; this sense is larger than perceived benefit.
- People are often scared of sharing failures, there does not exist a culture of innovation where small failures are learned from and people can move onwards smarter.
- How do practitioners know the "organizational readiness" of an agency for the change being implemented?
- Some people are afraid that they will be looked down on for not knowing new trends or technologies.
- Change is constant and adoption can be slow.

Best Practices and Lessons Learned The session offered the following best practices and lessons learned. The themes developed help promote collaboration, and overcome challenges such as the status quo bias.

- Create and use collaboration mechanisms
- Operationalizing a culture in the agency where continued learning is the norm
- Support is needed both from top-down (i.e., executive level) and bottom-up (i.e., people willing to learn and support each other)

- White papers can inform policy and should be encouraged
- Develop and share use cases (inter-agency, cross-agency)
- Provide teaching/learning opportunities. Example lessons learned include the following:
  - acquisition process ideas
  - emerging technologies
  - processes – changes and successes

Recommendations Leadership, communication, organizational readiness, and change management play key roles in IT modernization initiatives and must not be overlooked. The Booz Allen and Hamilton article concludes:

> As federal agencies look to move forward with IT modernization initiatives, they should build in change management as a key component to their plans. All too often, it's an overlooked piece of the puzzle, or agencies feel that they don't need to invest in change management (or the first to get cut when budgets are tight).

The session participants deliberated these issues and offered the following recommendations along very similar lines:

- Start with working groups
- Find executive sponsors who are willing to be vocal
- Increase communication:
  - need structure
  - multi-channel – calls, papers, blogs, all forms
- Need facilitation to keep the group together and move along
- Make information
  - consumable: both in graphics and words
  - accessible: a SharePoint site cannot be accessed by industry or other agencies
- Stop punishing failures and start celebrating wins
- Prepare to change/augment your organization (officially and unofficially); change within the confines of your agency

3.3.3.3 Data and Analytics Discovery, analysis, and communication of meaningful patterns of data, and their application in effective decision-making, play an ever-increasing role in agency IT modernization initiatives. According to a McKinsey article[11], "big data and analytics are helping businesses to become smarter, more productive, and better at making predictions." The data and analysis session deliberated and offered the following challenges and opportunities, best practices, and recommendations.

Challenges As with many topics related to IT modernization, some of the challenges are specific to the topic, and others, common across the topics. The McKinsey article calls out three specific challenges associated with data and analytics: Which data to use, handling analytics, and using the insights gained to transform operations. The Data and Analytics session deliberations identified several general and topic-specific challenges.

- Data and analytics initiatives often lack common objectives (e.g., as a one-page vision with articulated outcomes).
- Geospatial accuracy, particularly with unstructured data, is often a challenge.
- Transformation initiatives often use legacy systems, are half-done, and then lose budget.
- Legal assessments with geospatial intelligence often limit their use.
- Budget to fully clean up the data is often lacking.
- Correlation of disparate data is often a challenge.
- Lack of articulation of what the finish line looks like often hinders progress.
- Definitive identity management; definitive privacy are often difficult.
- Data quality is a challenge.

Best Practices and Lessons Learned In an article titled "Five Best Practices for Data Analytics,"[6] the online site IT Toolbox offers the following: (1) Starting with the end in mind (2) Building an Analytics culture (3) Reengineering data systems for analytics (4) Focus on useful data islands and (5) Iterate often. The challenges posed in government agencies are often complex due to the vast quantities of data, data diversity, and legacy systems that were built before the advent of big data.

The participants in the session took these factors into consideration and offered several best practices and lessons learned.

- Dashboard visualization is an important aspect of data and analytics.
- Development of minimally viable products is helpful in validating learning and continued development.
- Focusing on mission may help break silos and enable progress.
- Set vision and clearly articulate outcomes.
- Having early adopters, like minimally viable products, is important to success.
- Using effective change management techniques is a key ingredient to success.

Recommendations Given the set of challenges and best practices, not surprisingly, the recommendations that came out of the session focused on both cultural and technical aspects, and are listed below.

- Begin with the end in mind.
- Both anecdotal successes as well as quantified success metrics are important and should be adopted.
- Have agile (fully) in mind; develop minimally viable products along the way; identify early adopters.

3.3.4 Session Recommendations

The collaboration session on IT Modernization had breakout sessions on Cloud Adoption, Culture, and Data and Analytics. Some overall recommendations from those sessions are shown below.

With respect to Cloud Adoption:

- Create working groups across agencies to ensure broad acceptance
- Include mission folks and security folks in working groups with IT
- Change needs to come from the top
- Transition adoption needs to get more attention in Requests for Proposals (RFPs)

- Let the marketplace decide the winner – The government needs to provide clear requirements and desired outcomes

With respect to IT Modernization and Culture

- Start with working groups
- Find executive sponsors who are willing to be vocal
- Increase communication
- Facilitation is required to keep the group together and moving along
- Make information consumable and accessible
- Stop punishing failures and start celebrating wins

With respect to Data and Analytics

- Begin with the end in mind
- Both anecdotal successes as well as quantified success metrics are important and should be adopted
- Use agile development practices: identify minimally viable products along the way; identify early adopters

4 RECOMMENDATIONS

Some common recommendations emerged from the diverse set of collaboration sessions. The participants from government, academia, industry, and federal funded research and development centers identified recommendations from several of those sessions.

Get a champion. Get senior executive sponsorship as early as possible in the modernization process. Develop road maps and technology landscapes. Understand your data and practices.

Invest in data. Identify datasets that would benefit from widespread availability. Implement CRM to capture customer feedback to improve experience and relevance.

Invest in artificial intelligence and machine learning. Automate as much as possible. Start small and scale up (e.g., by identifying repeatable tasks that can easily be automated). This will help empower staff with more enriching and impactful work.

Invest in staff. Make sure staff is adequately trained and that they have ample opportunities for continuous training. These technologies (e.g., cloud, cyber, and – particularly – AI) are quickly evolving. Even if implementation of the technologies can be performed or outsourced, technical competency by government staff is required for envisioning, managing, and monitoring this work. Capture staff knowledge. Use automation to increase their effectiveness, skill, and satisfaction which will lead to retention and define the return on investment from training.

5 CONCLUSIONS

The collaboration sessions at the Government Information Technolog (GITEC) conference focused on three different areas of emerging technology that are important across the government: security, digital experience, and IT modernization. An enthusiastic group of experts in these and other areas converged to dive into various aspects of these areas. The security session had seven different breakout sessions, while digital experience and IT modernization had two and three break out sessions, respectively, Running so many simultaneous sessions, capturing the essence of those discussions, and synthesizing a coherent report from those diverse pieces was challenging. However, some themes and recommendations emerged, as presented in the previous section. Future conferences, though, should focus on fewer topics while encouraging greater participation and input.

REFERENCES

[1] 113th Congress. Federal Information Technology Acquisition Reform Act (FITARA). https://www.congress.gov/bill/113th-congress/house-bill/1232, 2014.

[2] ACT-IAC. Zero Trust Cybersecurity: Current Trends. Technical report, ACT-IAC, 2019.

[3] Department of Homeland Security. Federal information security modernization act (fisma). https://www.dhs.gov/fisma, 2016.

[4] Federal Network Resilience. Trusted Internet Connections (TIC) Reference Architecture Document Version 2.0. Technical report, Department of Homeland Security, 2013.

[5] GSA. Government-wide IT Accessibility Program. https://www.section508.gov/, 2020.

[6] P. Kowalke. Five Best Practices for Big Data Analytics. https://it.toolbox.com/blogs/erpdesk/five-best-practices-for-big-data-analytics-100316, 2016.

[7] S. Majendran. Organizational challenges in cloud adoption and enablers of cloud transition program. Technical Report Working Paper CISL 2013-13, The MITRE Corporation; The Advanced Technology Academic Research Center, 2013.

[8] NIST. Security and Privacy Controls for Federal Information Systems and Organizations. Technical Report Special Publication 800-53, National Institute of Standards and Technology, 2018.

[9] M. J. Spina, D. B. Faatz, D. S. Weitzel, R. S. Paul, T. A. Teter, L. F. Wilcox, N. G. Parrish, J. F. Brunelle, and T. Suder. March 2019 federal ciso summit report. Technical report, The MITRE Corporation; The Advanced Technology Academic Research Center, 2019.

[10] The Advanced Technology Academic Research Center. ATARC Announces Merger with GITEC.

[11] The Advanced Technology Academic Research Center. ATARC Cloud Innovation Lab.

[12] The MITRE Corporation. FFRDCs – A Primer. http://www.mitre.org/sites/default/files/publications/ffrdc-primer-april-2015.pdf, 2015.