Research Portfolio on Social Security's IT Modernization

IT Speaker Series Summary, 2021 – 2022

Social Security Advisory Board
December 2022

Bob Joondeph, Chair
Nancy J. Altman
Jagadeesh Gokhale
Amy Shuart

SOCIAL SECURITY
SSAB
ADVISORY BOARD

Table of Contents

Acronym List

AAL	Authenticator Assurance Level
AI	Artificial Intelligence
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Category Management
COBOL	Common Business-Orientated Language
COTS	Commercial Off the Shelf
CSP	Common Services Provider
CX	Customer Experience
DevOps	Development and Operations
DevSecOps	Development, Security, and Operations
EO	Executive Order
EX	Employees' Experience
FAS	Federal Acquisition Services
FedRAMP	Federal Risk and Management Program
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GAO	Government Accountability Office
GSA	General Services Administration
IAL1	Identity Assurance Level One
IAL2	Identity Assurance Level Two
ITC	Information Technology Category
ML	Machine Learning
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
RPA	Robotic Process Automation
SSA	Social Security Administration
SSI	Supplemental Security Income
VA	Veterans Affairs
VEO	Veteran's Experience Office
ZT	Zero Trust

Introduction

In 2017, the Social Security Administration (SSA) published its IT Modernization Plan, a five-year, $691 million[1] investment[2] in IT modernization. SSA's IT Modernization Plan covered the agency's legacy systems upgrades, streamlining agency workload processing and modernizing public service provision.[3] SSA published its IT Modernization Plan Update[4] in 2020, expanding the 2017 plan, including adding a new Service Delivery domain, refining its governance, and revising agency IT project roadmaps.

Appreciating the importance of disciplinary expertise and the critical role of IT modernization to SSA's mission and strategic plan, the Social Security Advisory Board ("Board") commissioned an independent panel of IT systems experts to provide guidance and advice on SSA's IT modernization efforts. The Panel's report[5] evaluated SSA's 2017 plan, the 2020 update, and the agency's organizational approach to IT modernization. In addition, the Panel met with current and former SSA leaders and employee groups, including systems end-users, advocacy groups, and other experts relevant to SSA's IT modernization.

Following the release of the Panel's final report, the Board continued its interest in SSA's IT modernization efforts and established a public IT Systems Speaker Series ("Speaker Series"). From fiscal year 2021 (FY 21) through FY 22, the Board recruited experts to present on a wide range of IT modernization-related topics. The presentations include the history of SSA's IT systems development, digital identity, legacy systems modernization, customer experience, cybersecurity, IT acquisition, and systems security and usability.

The Board's website hosts the complete Speaker Series video presentations and supporting materials. This paper summarizes key presentation information and themes presented for convenience. To improve the usefulness of summary content, we include footnotes defining key terms and provide a glossary of

---

[1] The initial investment of SSA'S IT Modernization Plan was estimated at $677 million and was later increased to $691 million.
[2] US House of Representatives, House Ways and Means Subcommittee on Social Security, *ICYMI: Subcommittee Examines Social Security's IT*, October 2018.
[3] SSA, *IT Modernization Plan: A Business and IT Journey*, October 2017 and Social Security Administration, *Service Modernization: IT Modernization Plan, 2020 Update*, June 2020.
[4] SSA, *Service Modernization: IT Modernization Plan, 2020 Update*, June 2020.
[5] SSAB, IT Systems Expert Panel, *Essential Changes Imperative for the Success of Social Security's IT Modernization and Future Operations*, December 2020.

terms at the end of the paper. Following the Speaker Series summaries,[6] we highlight examples of key presentation themes related to the expert IT Panel's final report. The Board-commissioned IT Panel and Speaker Series represent a diverse collection of disciplinary and institutional expertise, helpful for those engaged in federal IT modernization initiatives, particularly those efforts underway at SSA.

Session 1 – Historical Overview of Social Security's IT Systems

January 28, 2021

Renny DiPentima, former Deputy Commissioner of Systems, SSA; member of the Board-Commissioned IT Systems Expert Panel (2019-2021)

Alan Balutis, Distinguished Fellow and Senior Director of North American Public Sector, Cisco Systems' Business Solutions Group (*retired*); Chair of the Board Commissioned IT Systems Expert Panel (2019-2021)

Session Summary

DiPentima provided a historical summary of SSA's IT systems that were developed in 1935-1937 and continue to influence the systems used today. Independently designed and operated, systems were organized around Social Security numbers, earnings, and the master beneficiary record system.[7] Due to a lack of integration, SSA still maintains beneficiary records in multiple siloed systems.[8] DiPentima described SSA's early systems modernization efforts (through the 1970s-1980s) to improve agency data processing speeds, increase business process efficiencies for SSA employees and improve the customer experience.

---

[6] Please note: For reader convenience, terms defined in footnotes are also included in the glossary of terms found in the appendix.

[7] SSA defines the Master Beneficiary Record as "a SSA system containing information about each claimant who has applied for retirement, survivors, or disability benefits or who is to be enrolled in the Hospital Insurance or Supplementary Medial Insurance program." Further information can be found in: Dotty O'Brien, Joel Packman, and Carolyn Puckett, *Use of SSA's Data for Research Purposes*, SSA, *Social Security Bulletin* 65, no. 2, 2003/2004, last accessed December 1, 2022.

[8] SSA refers to its siloed systems in its IT Modernization Plan. SSA, *IT Modernization Plan: A Business and IT Journey*, October 2017.

SSA's earliest automation[9] used IBM machines for retirement benefits calculations. They sped processing but necessitated massive teletype storage the size of football fields, with employees using golf carts to collect the tapes.[10] Record updating was also inefficient and labor-intensive. For example, if 100,000 transactions came into the system daily with 80 million total beneficiaries, all 80 million beneficiary records were processed to locate the 100,000 files necessitating updating. By the 1970s, SSA began experiencing systems-related challenges and persistent workload backlogs. Supplemental Security Income's (SSI) passage in 1972 highlighted systems weaknesses[11] which worsened by 1974-1975. A primary weakness was the quick processing time SSI applications necessitated for applicants with immediate needs (whereas retirement applications afforded SSA 60-120 days to process benefits). Congressional concern motivated SSA's first IT Modernization Plan in 1982.[12] Congress provided $454 million for the plan,[13] which focused on customer preferences and divided into Survival, Transition, and State of the Art phases,[14] which included (but were not limited to) the following activities:[15]

- Replacing teletypes with online data
- Establishing a workstation network to replace the teletype data
- Using computers with greater processing power to support the system
- Creating a new data center with modern data processing
- Developing new software systems for modernizing claims processing

---

[9] Please see Larry DeWitt, "*Early Automation Challenges for SSA*," SSA Historian's Office, Research Note #6, April 2000, for additional information.

[10] For additional information about SSA's systems development history and automation challenges see: SSA, *Operating Methods: Establishment of the Total Data Systems Plan for Integration of Claims Processes*, Social Security History, History of SSA During the Johnson Administration 1963-1968, last accessed December 2, 2022.

[11] For more information on SSA's IT systems crisis in the 1970s and early 1980s see: US Congress, Office of Technology Assessment (OTA), "Deepening Problems, 1972-1981," in *The SSA and IT: Special Report*, OTA-CIT-311 (Washington, DC: Government Printing Office (GPO), October 1986), 103-116.

[12] Further information about SSA's 1982 Systems Modernization Plan is found in US Congress, OTA, *The SSA and IT: Special Report*, OTA-CIT-311 (Washington, DC: GPO, October 1986).

[13] For expert testimony regarding SSA's 1982 Systems Modernization Plan, see: General Accounting Office, "Statement of Michael Zimmerman, Director of Human Resource Information Systems, Information Management and Technology Division before the Committee on Ways and Means, House of Representatives," GAO-T-IMTEC-89-11, *SSA's Systems Modernization Plan*, September 28, 1989.

[14] For further information on activities undertaken during SSA's 1982 Systems Modernization Plan see: OTA, OTA-CIT-311, Figure 2.

[15] For additional information about the initial phases of SSA's 1982 Systems Modernization Plan see: US Congress, OTA, *The Beginning of the Systems Modernization Plan, 1982*, in *The SSA and IT: Special Report*, OTA-CIT-311 (Washington, DC: GPO, October 1986), 119-131.

SSA systems developed under the plan were online, interactive, and user-friendly. They implemented in phases with pilot testing and included cross-agency stakeholders in the process. Employees also had immediate access to headquarters' data. SSA continued using business-driven, customer-oriented strategies and worked toward integration with other federal agencies.[16] These systems are still used today as SSA's current legacy systems.

After DiPentima concluded his presentation, Alan Balutis discussed SSA's 2017 IT Modernization Plan[17] and the 2020 Modernization Plan Update. Balutis highlighted how the 2017 Plan included short and long-term initiatives to update agency IT hardware and software, while the 2020 Update prioritized the customer experience in the IT modernization efforts.[18] Balutis also highlighted SSA's transition to remote work due to the COVID-19 pandemic. Roughly 18,000 employees teleworked periodically pre-pandemic compared to more than 60,000 remote-working daily post-pandemic, resulting in strain on the agency's IT systems.

Session 2 – Digital Identity

March 26, 2021

Login.gov Perspective

> **Phil Lam,** Executive Director of Identity, Technology Transformation Services, General Services Administration (GSA)

Session Summary

Phil Lam discussed GSA's shared IT services. Its acquisition solutions offer private sector professional services, supplies, equipment, and IT to government agencies, promoting management best practices and efficient government operations. GSA's Technology Transformation Services office aims to help

[16] For more information about SSA's 1982 Systems Modernization Plan and ongoing IT systems modernization efforts see: OTA, OTA-CIT-311; US Congress, OTA, *SSA's Decentralized Computer Strategy: Issues and Options*, OTA-TCT-592 (Washington, DC: GPO, April 1994).
[17] SSA, *IT Modernization Plan: A Business and IT Journey*, October 2017.
[18] SSA, *Service Modernization: IT Modernization Plan, 2020 Update*, June 2020.

partners modernize. Identity authentication[19] and verification[20] are foundational to this goal.

Using Office of Management and Budget (OMB) guidance 19-17,[21] GSA facilitates identity verification across government and private sector partners. Login.gov,[22] one of GSA's premier products, is a single sign-on web interface providing strong identity verification services to federal agencies. GSA has over 27 million Login.gov users and 130 million identity authentications processed annually across 150 live sites and more than 20 federal agencies.[23] Login.gov complies with the US National Institute of Standards and Technology[24] (NIST) Special Publication 800-63-3 guidelines[25] which detail technical requirements for federal agencies implementing digital identity services. Login.gov is also Federal Risk and Management Program[26] ("FedRAMP") authorized, complying with security certification for common services providers[27] (CSP) offering cloud[28] services to federal agencies. Finally, Login.gov is a Federal Information

[19] NIST defines identity authentication as "verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system." Department of Commerce (DOC), NIST, "Authentication," last accessed December 1, 2022.
[20] NIST defines verification as "the process of confirming or denying that a claimed identity is correct by comparing the credentials of a person requesting access with those previously proven and associated with the PIV Card or a derived PIV credential associated with the identity being claimed." DOC, NIST, "Verification," last accessed December 1, 2022.
[21] Russell T. Vought, *Re: Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, Office of Management and Budget, Memorandum 19-17, May 21, 2019.
[22] For more information see: Login.gov
[23] Statistics as reported by Lam during this public session in March 2021.
[24] For more information see: nist.gov
[25] Paul A. Grassi, Michael E. Garcia, and James L. Fenton, *Digital Identity Guidelines*, DOC, NIST, Special Publication 800-63-3, June 2017.
[26] FedRAMP is "a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP empowers agencies to use modern cloud technologies, with emphasis on security and protection of federal information, and helps accelerate the adoption of secure, cloud solutions." GSA, "FedRAMP," last accessed December 1, 2022.
[27] CSP is "a federal organization that provides National Security System-Public Key Infrastructure (NSS-PKI) support to other federal organizations, academia and industrial partners requiring classified NSS-PKI support but without their own self-managed infrastructures." DOC, NIST, "CSP," last accessed December 1, 2022.
[28] The cloud refers to servers that are accessed over the Internet, and the software and databases that run on those servers. The cloud enables users to access the same files and applications from almost any device, because the computing and storage takes place on servers in a data center, instead of locally on the user device. By using cloud computing, users and companies do not have to manage physical servers themselves or run software applications on their own machines. Information taken from: Cloudfare, "What is the Cloud?," last accessed December 1, 2022.

Security Modernization Act (FISMA)[29] moderate system meaning it meets information security standards required for federal agencies and contractors. Overall, Login.gov simplifies online government services access and reduces agency costs and complexities.

Identity verification can be challenging for agencies as the process requires sharing data. Data sharing is problematic because there is an increased risk when maintaining personally identifiable information (PII)[30]. Many agencies check data with credit bureau partners and are reluctant to expose their data. To reduce PII sharing, GSA builds real-time[31] data exchange capabilities without data storage and verifies identity via "yes" or "no" to PII questions. In addition to providing identity verification services with Login.gov, GSA also aims to unite agencies by expanding its other services, specifically accreditation, innovation, and acquisition services. Duplication occurs when each agency must determine if vendors meet the NIST standards and federal requirements. GSA can provide a central vendor accreditation service and shared contracts supporting agencies' acquisitions to alleviate duplication of efforts. Finally, GSA also supports agencies by pooling resources, piloting programs, and communicating outcomes to increase visibility across agencies and support innovation.

ID.me Perspective

Blake Hall, Co-Founder and CEO, ID.me

Session Summary

Blake Hall gave an overview of ID.me, a company providing identity verification services and fighting identity fraud for over 39 million members.[32] ID.me is

[29] Federal Information Security Modernization Act of 2014, Pub. L. no. 113-283 (December 18, 2014); For more information see: Cybersecurity & Infrastructure Security Agency (CISA), "FISMA," last accessed December 1, 2022.
[30] Personally identifiable information (PII) is "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." DOC, NIST, "PII," last accessed December 1, 2022.
[31] Real-time is defined as "pertaining to the performance of a computation during the actual time that the related physical process transpires so that the results of the computation can be used to guide the physical process." DOC, NIST, "Real-Time," last accessed December 1, 2022.
[32] Statistics as reported by Hall during this public session in March 2021.

NIST 800-63 certified, FedRAMP authorized, and undergoes independent auditing. It makes secure identity services accessible for consumers and easy to integrate for agency partners. Mentioned as the first US-based identity network making digital credentials portable, ID.me focuses on login credentials and identity verification.

COVID-19 accentuated the digital economy's[33] explosion as identity verification moves from knowledge-based to possession and biometric-based methods. Identity verification underpins societal transactions (e.g., education, healthcare, employment, etc.). ID.me offers three identity proofing methods: online self-service (meeting NIST 800-63-3 IAL2 standards),[34] proofing via virtual means, and in-person proofing. ID.me users can configure validation, verification, and multi-factor authentication[35] by their needed level of legal ID proofing, while government and healthcare organizations must meet NIST 800-63-3 IAL2/AAL2[36] standards. Users of ID.me services control their own data post-authentication/verification. Finally, ID.me employs multiple resources, including accessing multiple credit bureaus' data to support verification, validation, and multi-factor authentication.

Passwords were already unsustainable, so requiring identity authentication and multi-factorial login verification at one organization may create friction for the user - and higher costs for the organization. ID.me verifies the user once with multiple organizations, improving security and reducing costs. Their services are cost-effective; the government does not pay a per-user login.

---

[33] Digital economy is "the economic effects of online shopping, digital media, the sharing economy, and other e-commerce developments are captured within GDP and other BEA statistics." Bureau of Economic Analysis, "Special Topics," last accessed December 1, 2022.
[34] NIST 800-63-3 identity assurance level 2 (IAL2) standards require evidence supporting the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically-present identity proofing. This is contrasted with IAL1, which has no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the subject's activities are self-asserted or should be treated as self-asserted, which are neither validated nor verified. For more information about NIST identity assurance levels see: Paul A. Grassi, Michael E. Garcia, and James L. Fenton, *Digital Identity Guidelines*, DOC, NIST, Special Publication 800-63-3, June 2017, last accessed December 1, 2022.
[35] Multi-factor authentication (MFA) is "authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric)." DOC, NIST, "MFA," last accessed December 1, 2022.
[36] The authenticator assurance level (AAL) "is a measure of the strength of an authentication mechanism and, therefore, the confidence in it, as defined in [NIST SP 800-63-3] in terms of three levels: AAL1 (Some confidence), AAL2 (High confidence), AAL3 (Very high confidence)." DOC, NIST, "AAL," last accessed December 1, 2022.

Between October 2020-March 2021, there was over 900 percent increase in dark web traffic related to ID.me, and ID.me addressed multiple types of fraud. Over 200 million Americans already have exposed data due to numerous breaches (e.g., Equifax, OPM, Solar Winds, T-Mobile). Cyber attack vectors[37] include primary social engineering fraud (when legitimate identity owners unwittingly help the attacker perpetrate fraud), fraudulent document use, and breached PII. Ohio, New York, Illinois, Kansas, and Maryland were hit hard with fraudulent Social Security attacks when attackers used state systems to harvest victims' PII.

Session 3 – Modernizing Legacy IT Systems

May 21, 2021

Kevin C. Walsh, Director of Information Technology and Cybersecurity, Government Accountability Office

Robert Klopp, Owner/Principal, Skyland Digital Services; former Deputy Commissioner for Systems and Chief Information Officer, SSA

Session Summary

There is no clear legacy system definition, explained Kevin Walsh. Its attributes include lacking vendor support for hardware, software, or programming code or no longer meeting mission needs. Rob Klopp added that a legacy system exists when there is a significant difference between a current and modern system.[38]

[37] An attack vector is "a pathway or method used by a hacker to illegally access a network or computer in an attempt to exploit system vulnerabilities. Hackers use numerous attack vectors to launch attacks that take advantage of system weaknesses, cause a data breach, or steal login credentials." Fortinet, "What is an Attack Vector," last accessed December 1, 2022.
[38] Another definition of a legacy system is "an information system based on outdated technologies and critical to day-to-day operations." Replacing and modernizing legacy applications and systems with new and different technologies is a significant challenge. As organizations modernize their IT, they must ensure the new technology is compatible with older systems and data formats (until they can be fully modernized or replaced). For more information on legacy systems see: Sygma Technology, "What Are Legacy Systems," last accessed December 1, 2022.

According to Klopp, technical debt[39] is the gap between modern systems technology and an agency's current technology. Agencies reduce this debt via continuous improvement and integration, but it accrues rapidly due to the pace of technology change. Walsh explained that technical debt challenges the government; agencies cannot always pre-plan modernization activities due to the federal budget process for IT investment. Klopp recommended the government should change funding approaches and accountability measures.

Modernization is not always a money saver, but Walsh and Klopp agreed that it is critical to stay current. Doing so begins with organizational culture change and agency leadership prepared to make controversial decisions. Staying current in IT will challenge agencies until culture change supports continuous IT business process improvement and evaluation. Walsh said agencies modernize by updating older systems with newer hardware and software or by adding minimally customized commercial-off-the-shelf software (COTS)[40] packages. Klopp described programmers' openness in Silicon Valley to learning new programming languages and using different database management systems. Similarly, agencies should consider new database management systems every two to three years and assess programming language use for each project. Klopp believes contractors develop skills based on agency needs - and can support them with immersive, intensive boot camps to keep agency skills current.

[39] Technical debt (also known as "tech debt" or "code debt") implies costs from choosing an easy (or limited) IT solution now - instead of using a better, longer-term solution. There is a tradeoff between the short-term benefits of rapid delivery and the long-term value of developing a software system that is easy to evolve, modify, repair, and sustain. Like financial debt, technical debt can be a burden or an investment. Splunk, "What is Tech Debt," last accessed December 1, 2022; Carnegie Mellon University, Software Engineering Institute, "Managing Technical Debt with Data-Driven Analysis," February 2022.

[40] NIST defines commercial-off-the-shelf (COTS) as "a software and/or hardware product that is commercially ready-made and available for sale, lease, or license to the general public." Department of Commerce, NIST, "COTS," last accessed December 1, 2022.

SSA typically modernizes by releasing new modules[41] rather than rewriting the core language (60 million COBOL[42] lines/seven million Assembly[43] lines run its core legacy systems). Modules must be carefully designed not to affect the main system; otherwise, technical risk and integration costs increase more than if developed from scratch. Klopp noted updating an outdated programming language still residing on old system architecture is not a modern system. As SSA's former CIO, Klopp led the development of a new disability case processing system (DCPS2). Business needs drove program development, and they modernized the simplest cases first using agile[44] and DevSecOps[45] methodologies. Smaller steps facilitated the release of usable portions and earlier receipt of customer reactions.

Agencies must incorporate cybersecurity throughout IT systems and regularly consider risks. SSA has a cyber structural advantage since it is a more centralized IT organization (decentralized, fragmented systems have increased cyber threats). Also, SSA's CIO controls the agency's entire network with contained, centralized systems.

When asked about measuring IT progress, Klopp recommended two major IT functions: software development and maintenance evaluation. Staying current with vendor-used programming languages and measuring distance from the

---

[41] A Module is any of a number of distinct but interrelated units from which a program may be built up or into which a complex activity may be analyzed. Testapedia, "Module," last accessed December 2, 2022.

[42] Common Business-Orientated Language (COBOL) is a high-level computer programming language first used in the 1960s and was very popular in the business community. COBOL's popularity began declining in the 1990s and it is now considered an outdated programming language, often the programming language (or code) of legacy systems. Although considered outdated, COBOL is still in use today. For more information about COBOL see: Smithsonian, National Museum of American History, "COBOL," last accessed December 1, 2022; Patrick Stanard, "Today's Business Systems Run on COBOL," *TechChannel*, March 10, 2021.

[43] Assembly language, also known as assembler language, is a low-level programming language that is designed to communicate instructions with specific computer hardware and direct the flow of information. Megha Thakkar, "What is Assembly Language? A Quick Overview," *InfoSec Insights by Sectigo Store*, May 3, 2022.

[44] Agile software development is "a group of software development methodologies based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams." CISCO, *Agile Product Development at CISCO: Collaborative, Customer-Centered Software Development*, White Paper, 2011.

[45] Development, Security, and Operations ("DevSecOps") "automates the integration security at every phase of the software development lifecycle, from initial design through integration, testing, deployment, and software delivery." This is contrasted with past approaches where security was added on at the end of the development cycle, often by a separate security team. IBM Cloud Education, "What is DevSecOps?" IBM, July 30, 2020.

latest software release are possible software development and maintenance measures. Costs divided by business transactions evaluate operational or infrastructure expenses (ideally, the cost per transaction will decrease over time). One could consider the number of staff required to process a specific number of cases to measure usability. Agencies can use these metrics to measure IT progress and modernization and incentivize cloud transitioning.

Session 4 – Customer Experience

July 30, 2021

Barbara C. Morton, Deputy Chief Veterans Experience Officer, Veterans Experience Office, Department of Veterans Affairs

Session Summary

Barbara Morton described the VA's customer experience (CX) initiative and how the 2014 Phoenix Office of Inspector General (OIG) report[46] reinforced its need to invest in CX. By 2015, the VA established the Veteran's Experience Office (VEO),[47] headed by the Chief Veterans Experience Officer, reporting directly to the Secretary. Key CX accomplishments are a redesigned website,[48] a Welcome Kit,[49] and a CX Cookbook.[50]

The VA's CX Framework[51] showcases agency-wide initiatives applicable to other federal agencies. Modeling after the private sector, the VA implements CX using data, tools, technology, and engagement along three pillars of its CX Strategy: Core Capabilities & Framework, CX Governance, and CX Accountability. The VA also institutionalized CX in policy and operational decision-making. Customer trust increased from 55 percent in 2016 to 79 percent in 2021, as measured by its VA-wide trust survey.[52]

---

[46] VA Office of Inspector General, *Veterans Health Administration: Review of Alleged Patient Deaths, Patient Wait Times, and Scheduling Practices at the Phoenix VA Health Care System-14-02603-267,* August 26, 2014.
[47] For further information about the VEO see: VA, "Veterans Experience Office (VEO)," last accessed December 1, 2022.
[48] For more information see: va.gov.
[49] For the VA Welcome kit see: VA, "Print Out Your VA Welcome Kit," last accessed December 1, 2022.
[50] Veterans Affairs (VA), VEO, *The Customer Experience (CX) Cookbook,* November 11, 2020.
[51] See: VA, VEO, *VA's CX Framework*, last accessed December 1, 2022.
[52] For more information about the VA's VA-wide trust survey and other key VA CX indicators see: VA, *Veterans Experience with VA.gov: FY 2020 Q4 Update*, 2020.

The VA's CX Cookbook[53] is a multi-faceted framework to help agencies establish and build CX in their organizations. It guides agencies to "adapt and adopt" CX best practices from the government and the private sector and includes journey maps. VA journey maps[54] align services to moments that matter most to veterans, which do not always appear on traditional operational dashboards. The VEO created 45 unique journey maps and accompanying reports to prototype and deploy tangible CX tools and products. They also address VA employees' experiences (EX), creating the VA's first-ever[55] EX journey map.[56]

CX also supports IT modernization. The VA modernized digital services to ease veterans' access to services online. It also relaunched VA.gov with feedback to provide a single digital location to access all VA services in one place. These changes resulted in a 20 percent increase in user satisfaction and a 221 percent increase in average monthly website users.[57] The VA is also modernizing its VA Contact Center software platform so veterans can update their contact information across all VA and Veterans Benefits Administration systems in one place. Other modernization investments include digital and real-time data collection using human-centered design to gather important insights. Morton concluded by providing resources and references for agencies to develop and strengthen their CX initiatives.

Session 5 – Federal Cybersecurity Landscape

November 19, 2021

An Update on Federal Information Technology and Cybersecurity Policies

---

[53] VA, VEO, *CX Cookbook*, November 11, 2020.
[54] A journey map is "a visualization of the major interactions shaping a user's experience of a product or service. To provide design teams with a bird's-eye view of a service that helps them see the sequence of interactions that make up a user's experience including the complexity, successes, pain points, and emotions users experience from the earliest phases of researching a product or service all the way through adoption." GSA, 18F Methods, "Journey Mapping," last accessed December 1, 2022. Also see Performance.gov, "Mapping the Cros-Agency Customer Experience," January 1, 2021.
[55] VA, "VA Creates Government's First-Ever Employee Experience Journey Map," December 22, 2020.
[56] VA, "VA Creates Government's First-Ever Employee Experience Journey Map," December 22, 2020.
[57] Barbara Morton, *CX*, VEO, Presentation to SSAB, July 30, 2021, Slide 18.

Dave Powner, Executive Director, Center for Data-Driven Policy, and Director, Strategic Engagement Partnerships, MITRE Corporation; former Director, Information Technology Management Issues, Government Accountability Office

Session Summary

Dave Powner began describing the federal cybersecurity landscape by reflecting on OMB's 2021 cybersecurity executive order (EO).[58] The EO calls on agencies to modernize their cybersecurity posture. It focuses on high-value assets, including zero trust architecture, securing the cloud, software supply chain, incident response, and ensuring software cybersecurity.

Zero Trust (ZT)[59] is fundamental to the EO. OMB released policies focusing on ZT architecture, and agencies need a clear ZT strategy. Vulnerability testing is important, as well as safe cloud application transfer. The earlier cyber strategy was "trust but verify" on perimeter defenses. "Never trust but verify every user, device, and application" as a collection of processes is the new approach.

Congress introduced cybersecurity legislation, including data collection (also an executive policy concentration) and reporting ransomware and cyber incidents. Another Congressional focus is legacy systems modernization to address the maintenance of archaic systems and security challenges. Powner emphasized the seriousness of large legacy applications tied to mission-critical operations: technical debt[60] rises annually, and security vulnerabilities are more exposed. Federal Information Security Management Act (FISMA)[61] reform

---

[58] *EO on Improving the Nation's Cybersecurity,* Executive Order 14028 (May 12, 2021).

[59] The National Security Agency (NSA) defines Zero Trust as "a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information fed from multiple sources to determine access and other system responses." NSA, *Embracing a Zero Trust Security Model*, February 2021.

[60] Technical debt (also known as "tech debt" or "code debt") implies costs from choosing an easy (or limited) IT solution now - instead of using a better, longer-term solution. There is a tradeoff between the short-term benefits of rapid delivery and the long-term value of developing a software system that is easy to evolve, modify, repair, and sustain. Like financial debt, technical debt can be a burden or an investment. Splunk, "What is Tech Debt," last accessed December 1, 2022; Carnegie Mellon University, Software Engineering Institute, "Managing Technical Debt with Data-Driven Analysis," February 2022.

[61] "FISMA requires federal agencies to implement a mandatory set of processes and system controls designed to ensure the confidentiality, integrity, and availability of system-related

focuses on post-incident activities and legacy systems modernization integration. Automating agency cloud security certification and proposed cyber metrics is also a focus. OMB-reported metrics differ from federal chief information security officer metrics.

Congress also has several customer experience (CX) bills impacting IT (CX is also a focus of the President's Management Agenda). Tying CX to the right outcome metrics ensures better mission outcomes, and IT plays a huge role. It is difficult to have good CX with archaic systems. Powner believes CX legislation should emphasize the importance of agencies aligning their IT strategy with agency strategic plans while collaborating with key players, including agency leaders across disciplines, and recommended legislation using CX data strategies. Powner also valued the Board-commissioned IT Systems Expert Panel Report's heavy CX emphasis and recommendations for IT modernization.[62]

A Foot in Both Camps: A Different Perspective on Cyber

> **Jim Richberg,** Public Sector Field CISO and Vice President, Information Security, Fortinet, Former US National Intelligence Manager, and Senior Advisor, US Director of National Intelligence

Session Summary

Jim Richberg described cybersecurity challenges, including increased attacks, data and solution overload, network surface vulnerability, cyber metrics, and workforce shortages. Skilled cybersecurity professionals are insufficient in number (three to four million people short) and often lack optimal skills. The amount of cybersecurity data is overwhelming. SSA's security operations center may have more than 75 cybersecurity tools reporting data for different cybersecurity problems. Employees must integrate the information and make sense of it, as most cybersecurity tools do not communicate with each other. The government does not understand all cyber trends well (e.g., the digital

---

information. The processes and systems controls in each federal agency must follow established Federal Information Processing Standards, National Institute of Standards and Technology standards, and other legislative requirements pertaining to federal information systems, such as the Privacy Act of 1974." GSA, "FISMA," January 24, 2018.

[62] IT Systems Expert Panel commissioned by the SSAB, *Essential Changes Imperative for the Success of Social Security's IT Modernization and Future Operations*, December 2020.

transformation[63]) and is often three to four years behind the curve. This is due to technical debt and an IT procurement cycle requiring up to five years. For over ten years, the cybersecurity industry has used artificial intelligence (AI)[64] and machine learning (ML)[65] to detect threats, and nearly all cybersecurity firms' threat detection is AI/ML generated. Still, neither the public nor private sector understands AI/ML and its human-machine interactions well.

COVID-19 dramatically accelerated government cybersecurity adoption - and changed service delivery. State and local governments rolled out robotic process automation (RPA),[66] like chat boxes. In January 2020, five to six states used RPA, and by June 2020, all states were using RPA. Richberg believes the hybrid work environment will continue, and most will not return to the office full-time. Of Richberg's personal surveys, 25 percent of employees prefer in-office work but not full-time. Many private-sector organizations are consolidating locations and changing office functions and new cybersecurity options are needed.

Richberg views SSA's IT modernization as an opportunity for the agency to implement a consistent cybersecurity philosophy across its systems. With a consistent cybersecurity philosophy, SSA can leverage automation and AI for efficiency and cost savings. A consistent philosophy can also help consolidate security and networking, prepare for ongoing technology changes (e.g., 5G and

---

[63] Digital transformation is "the process of completely replacing manual, traditional, and legacy ways of doing business with the latest digital alternatives across all aspects of business, not solely technology." Hewlett Packard Enterprise, "Digital Transformation," last accessed December 1, 2022.

[64] Artificial intelligence (AI) is "a branch of computer science devoted to developing data processing systems that performs functions normally associated with human intelligence, such as reasoning, learning, and self-improvement." Or it is "the capability of a device to perform functions that are normally associated with human intelligence such as reasoning, learning, and self-improvement." DOC, NIST, "AI," last accessed December 1, 2022. Also see: CISCO, "AI," last accessed December 1, 2022.

[65] Machine Learning (ML), a domain within the larger field of artificial intelligence, is described as letting "computers learn without explicit programming. It teaches computers to learn by experience". ML in security continuously learns via data analysis, finding patterns and better detecting malware, find insider threats, and predicting potential unsafe areas online to protect those browsing. It also can protect data in the cloud by detecting suspicious user behaviors. CISCO, "What is Machine Learning in Security?" last accessed December 1, 2022.

[66] "Robotic process automation (RPA), also known as software robotics, uses automation technologies to mimic back-office tasks of human workers, such as extracting data, filling in forms, and moving files." It can "also access information through legacy systems, integrating well with other applications through front-end integrations. This allows the automation platform to behave similarly to a human worker, performing routine tasks, such as logging in and copying and pasting from one system to another." IBM Cloud Education, "RPA," *IBM*, October 22, 2020.

edge computing[67]), and implement zero-trust principles and services, including cyber deterrence and defense approaches. Richberg noted agencies should spend smarter on cybersecurity, look for lessons learned from others, use the cybersecurity platform[68] approach, and develop trusted partnerships.

Session 6 – IT Acquisition

January 27, 2022

Laura Stanton, Associate Commissioner, Office of Information Technology Category (ITC), Federal Acquisition Service (FAS), General Services Administration (GSA)

Bill Zielinski, Chief Information Officer, City of Dallas; former Chief Information Officer, Social Security Administration (SSA)

Session Summary

Laura Stanton began by describing how category management (CM)[69] helps government obtain more value and savings.[70] The government has adopted CM, a commercial best practice for buying common goods and services, to find the best value, meet the government's small business goals, and ultimately save money for taxpayers.[71] Category management encourages competition and transparency, makes buying smarter, and builds a stronger government.[72]

---

[67] "Edge computing is a form of computing that is done on site or near a particular data source, minimizing the need for data to be processed in a remote data center, shifting computing resources from central data centers and clouds closer to devices." Hewlett Packard Enterprise, "Edge Computing," last accessed December 1, 2022; CISCO, "What is Edge Computing," last accessed December 1, 2022.

[68] "Security platforms integrate vendor-specific functions as well as third-party functions, allowing security teams to work more efficiently, faster, and more collaboratively by simplifying integration, improving visibility, sharing intelligence, and automating workflows across endpoints, cloud, network, and applications." CISCO, "What is a Security Platform," last accessed December 1, 2022.

[69] For further details about category management see: GSA, Great Government through Technology, "Tag: Category Management," last accessed December 1, 2022.

[70] For more information on category management see: Performance.gov Team, "Buy Smarter and Save Money with CM," August 13, 2019.

[71] Performance.gov, "CM: Leveraging Common Contracts and Best Practices to Drive Savings and Efficiencies," last accessed December 1, 2022.

[72] Performance.gov, "CM."

Government-wide spending in the last few years was over $600 billion on goods and services; over half were common goods but were often purchased individually. With IT spending of $70.6 billion in FY 21, GSA's Information Technology Category (ITC)[73] managed programs and contracts totaling $32 billion across five IT subcategories: IT hardware, software, security, services, and telecom. The ITC provides CM to 98 percent of federal agencies, plus state, local and tribal governments. More than half of the contracts were common[74] across federal agencies, frequently purchased individually by over 3000 buying offices and 40,000 contractors. GSA crafts acquisitions to serve a larger vision and relate to agency goals.

A priority[75] of the past three administrations, CM was initially launched around 2014-2015 and was part of the President's Management Agenda. A CM focus is assessing government spending with agencies-provided spending targets. In March 2019, OMB released the M-19-13,[76] a memo directing agencies to increase CM practices to improve agency outcomes.[77] Memo guidance addresses incorporating CM strategies for IT modernization, decentralized data and data accountability, and acquisitions into organized government contracting practices.

The presenters highlighted the numerous CM benefits, which include:

- Offering value for the industry
- Building more consistent requirements
- Improving understanding of the industry's commercial standards
- Reducing industry burden with government-wide contracts
- Facilitating innovation, and
- Analyzing how small business plays into the market

CM also helps GSA translate policies into action via government-wide frameworks and supports agency management actions advancing equity in

---

[73] For more information about GSA's Federal Acquisition Service Information Technology Category see: GSA, "Technology Products & Services: Overview," last accessed December 1, 2022; GSA, "GSA Schedule Offerings: MAS Categories," last accessed December 1, 2022.
[74] Examples of common services purchased by GSA's FAS include training, overnight delivery services, copier machines, travel, and many IT solutions.
[75] Jason S. Miller, *Re: Advancing Equity in Federal Procurement*, OMB, M-22-03, December 2, 2021.
[76] Margaret M. Weichert, *Re: CM: Making Smarter Use of Common Contract Solutions and Practices*, OMB, M-19-13, March 20, 2019.
[77] Memorandum M-19-13 was later amended and replaced by memorandum M-22-03.

procurement. CM develops IT acquisition intelligence capability on supplier and contract management and uses key performance indicators to reshape federal IT spending. GSA's contracts and services also support initiatives and assist with marketplace requirements to address executive orders (i.e., Buy American,[78] Cybersecurity,[79] Racial Equity[80]), including supporting cloud computing, cybersecurity, and small business utilization.

Stanton and co-presenter Bill Zielinski reviewed SSA's IT spending (FY 19-21),[81] highlighting that SSA entered into fewer contracts than other agencies but had the highest average dollars spent per IT contract.[82] SSA also uses more single-funded agency contracts than government-wide use (49 percent vs. 19 percent) and generally allocates a larger share of obligations to software (compared with the rest of the government—36 percent vs. 16 percent).[83] In FY 21, SSA ranked 11th of 90 departments and agencies for the highest dollars obligated but 16th in the number of contracts.[84] As a result, SSA had the highest average dollars spent per contract in the government.[85] This may have also contributed to SSA working with fewer small businesses (versus government-wide).[86] Zielinski mentioned the value of the Board's IT Systems Expert Panel Report, especially the CX recommendations for addressing IT.[87]

Session 7 – Making Secure Systems Easy for the Public to Use

February 16, 2022

[78] *EO on Ensuring the Future is Made in All of American by All of America's Workers,* EO 14005, January 25, 2021.
[79] *EO on Improving the Nation's Cybersecurity*, EO 14028, May 12, 2021.
[80] *EO on Advancing Racial Equity and Support for Underserved Communities Through the Federal Government*, EO 13985, January 20, 2021.
[81] Data Sources include Federal Procurement Data Source, (FPDS) obligation data as of 1/9/2022 and IT Dashboard IT investment data as of 12/12/2021 (original IT Dashboard pages are archived and no longer publicly available). See: Laura Stanton, *IT Category Management*, GSA, Office of IT Category, Presentation to SSAB, January 27, 2022.
[82] Laura Stanton, *IT Category Management*, GSA, Office of IT Category, Presentation to SSAB, January 27, 2022, 15.
[83] Stanton, *IT CM*, 15.
[84] Stanton, *IT CM*, 15, 19.
[85] Stanton, *IT CM*, 15.
[86] Stanton, *IT CM*, 15.
[87] IT Systems Expert Panel commissioned by the SSAB, *Essential Changes Imperative for the Success of Social Security's IT Modernization and Future Operations,* December 2020.

Lorrie Faith Cranor, Director and Bosch Distinguished Professor in Security and Privacy Technologies, CyLab and FORE Systems; Professor of Computer Science and Engineering and Public Policy, Carnegie Mellon University

Session Summary

Lorrie Cranor discussed making systems more usable while maintaining user security and privacy.[88] Cranor believes we should strive for systems' security and privacy while simultaneously maintaining usability.[89]

Passwords are an essential cybersecurity tool. However, most users re-use them due to difficulty remembering unique passwords. On average, users have 26 different accounts, ten different passwords, and re-use passwords across almost all website categories.[90] Due to re-use, attackers can easily determine predictable transformations of passwords when knowing prior passwords.[91] Research showed when online, attackers accessed 17 percent of accounts within five guesses.[92] When offline, attackers could access 41 percent of accounts within three seconds.[93] Cranor said we rely on users to perform security tasks they are not good at to keep systems secure, including creating and using memorable and unique passwords.[94]

Systems encourage or require users to change their passwords frequently, but the National Institute of Standards and Technology recommends against

---

[88] Research discussed in this presentation was funded in part by Carnegie Corporation of New York, Carnegie Mellon CyLab, DARPA, Facebook, Google, IBM, Microsoft Research, Innovators Network Foundation, NSA, NSF, PNC Center for Financial Services Innovation and the Privacy Project. See: Lorrie Faith Cranor, *Making Secure Systems Easy for the Public to Use*, Carnegie Mellon University, Cylab, Presentation to SSAB, February 16, 2022, Slide 101.
[89] Cranor, *Making Secure Systems Easy for the Public to Use*.
[90] For research cited by Cranor see: Sarah Pearman, Jeremy Thomas, Pardis Emani Maeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Alain Forget, "Let's Go in for a Closer Look: Observing Passwords in the Natural Habitat," *CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, October 2017, 295-310.
[91] For research cited by Cranor see: Yinqian Zhang, Fabian Monrose, and Michael K. Reiter, "The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis," *CCS '10 Proceedings of the 17th ACM Conference on Computer and Communications Security*, October 2010, 176-186.
[92] Zhang, Monrose, and Reiter, "The Security of Modern Password Expiration."
[93] Zhang, Monrose, and Reiter, "The Security of Modern Password Expiration."
[94] See: Carnegie Mellon University, *Tips for Creating a Strong Password*.

regular password expiration.[95,96] Instead, two-factor authentication and password management can help protect systems' security and privacy without negatively impacting usability. Password manager and generator adoption are low due to lack of awareness, underestimated risk of password re-use, confusing prompts, and usability and reliability problems. The research found that users of built-in password managers may be driven more by convenience, while users of separately installed password managers appear to be driven more by security.[97] Programmers should not ask users to perform security tasks where they lack proficiency; end-user testing of security and privacy changes to ensure user-friendly approaches is vital.

Connecting Session Themes with Recommendations from the Independent Board-Commissioned IT Panel

Lessons learned in this expert Speaker Series highlight important topics relevant to IT modernization. Additionally, many of the presenters' messages spanning multiple subjects relate to the IT Panel's report recommendations. We highlight several themes aligned with the Panel report's four IT recommendation categories below.[98]

Operating Model The Panel report states that an operating model[99] "is the organizing paradigm against which IT, policy, human resources, operations, and process decisions can be evaluated and understood."[100] The importance of

---

[95] Paul A. Grassi, Michael E. Garcia, and James L. Fenton, *Digital Identity Guidelines*, DOC, NIST, Special Publication 800-63-3, June 2017.

[96] Adam Clark Estes, "The Guy Who Invented Those Annoying Password Rules Now Regrets It," *Gizmodo*, August 8, 2017.

[97] For research cited by Cranor see: Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor, "Why People (Don't) Use Password Managers Effectively," *SOUPS '19: Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, August 2019, 319-338.

[98] Unless otherwise noted, statements summarize recommendations/statements of the IT Systems Expert Panel in their report: SSAB, IT Systems Expert Panel, *Essential Changes Imperative for the Success of Social Security's IT Modernization and Future Operations*, December 2020.

[99] The Panel also defines an operating model as "an abstract and visual representation or model of how an organization delivers value to its customers and beneficiaries – and how the organization works," is essential for any business, public or private, with a customer or citizen focus as the organizing principle." See: SSAB, IT Systems Expert Panel, *Essential Changes Imperative for the Success of Social Security's IT Modernization and Future Operations*, December 2020, 9.

[100] SSAB, IT Systems Expert Panel, *Essential Changes Imperative for the Success of Social Security's IT Modernization and Future Operations*, December 2020, 9.

an operating model informing IT modernization was a frequent topic of the IT Panel's meetings with various stakeholder groups.[101]

In session six of the Speaker Series, speakers Stanton and Zielinski discussed category management (CM),[102] a commercial best practice for buying common goods and services to obtain the best value, achieve the government's small business goals, and save taxpayer dollars.[103] CM can be helpful to federal agencies and aligns with multiple operating model recommendations.

Governance Infrastructure An enterprise-wide governance infrastructure is critical to support IT modernization consistency, agility, and excellence. It defines the modernization initiative's "what" and "how,"[104] and supports interrelated program management processes, collaboration with clearly defined roles, and decision-making processes.[105]

In session three, Walsh and Klopp presented on modernizing legacy systems and recommended using agile[106] and DevSecOps[107] methodologies to update legacy systems incrementally. They also discussed the importance of first starting with the simplest cases when modernizing IT systems. The discussion capitalized on government and agency-specific ideas and suggestions.

IT Modernization Strategy The Panel report states an IT modernization strategy is essential to modernize IT systems.[108] It should include internal and

---

[101] A complete listing of the Panel's operating model recommendations are available here: IT Systems Expert Panel, *Essential Changes Imperative for the Success of Social Security's IT Modernization and Future Operations,* 13.
[102] Performance.gov, "Buy Smarter and Save Money with CM," August 2019.
[103] Performance.gov, "CM: Leveraging Common Contracts and Best Practices to Drive Savings and Efficiencies," January 2021.
[104] IT Systems Expert Panel, *Essential Changes Imperative for the Success of Social Security's IT Modernization and Future Operations,* 13-17.
[105] A complete listing of the Panel's governance infrastructure recommendations are available here: IT Systems Expert Panel, *Essential Changes Imperative for the Success of Social Security's IT Modernization and Future Operations,* 16-17.
[106] Cisco defines agile software development as "a group of software development methodologies based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams."
[107] According to IBM, DevSecOps (short for development, security, and operations) "automates the integration security at every phase of the software development lifecycle, from initial design through integration, testing, deployment, and software delivery." This is contrasted with past approaches where security was added on at the end of the development cycle, often by a separate security team.
[108] A complete listing of the Panel's IT modernization strategy recommendations are available here: IT Systems Expert Panel, *Essential Changes Imperative for the Success of Social Security's IT Modernization and Future Operations,* 17-22.

external stakeholder contributions, connect SSA's IT modernization plans[109,110] and its 2018-2022 Strategic Plan[111,112] and define, akin to the governance structure, the modernization "how" and "what" in language agency executives can decipher, champion, and co-own.

In the Speaker Series' first session, DiPentima and Balutis described SSA's use of cross-agency stakeholder involvement and emerging technologies to enhance data stores in the agency's modernization efforts. During the fifth session of the Speaker Series on cybersecurity, Powner suggested using metrics to ensure better agency outcomes. Richberg, the second cybersecurity speaker, described the importance of using emerging technologies (e.g., artificial intelligence, [113] machine learning,[114] robotic process automation[115]) to enhance agency data stores.

Customer Experience The customer experience (CX) includes the governance or decision-making process for customer-focused initiatives and aligns IT investments and the organizational culture to customer needs.[116] CX also involves employees' commitment to customer-focused efforts, including data

---

[109] SSA, *IT Modernization Plan: A Business and IT Journey,* October 2017.
[110] SSA, *Service Modernization: IT Modernization Plan, 2020 Update*, June 2020.
[111] SSA's 2018-2022 Strategic Plan is available here. The most recent update is the agency's *2022-2026 Strategic Plan.*
[112] The Panel found a weak connection between SSA's strategic planning to its IT modernization plan execution. See p. 17 of IT Systems Expert Panel, *Essential Changes Imperative for the Success of Social Security's IT Modernization and Future Operations,* December 2020.
[113] Artificial intelligence (AI) is "a branch of computer science devoted to developing data processing systems that performs functions normally associated with human intelligence, such as reasoning, learning, and self-improvement." Or it is "the capability of a device to perform functions that are normally associated with human intelligence such as reasoning, learning, and self-improvement." DOC, NIST, "AI," last accessed December 2, 2022. Also see: CISCO, "AI," last accessed December 2, 2022.
[114] Machine Learning (ML), a domain within the larger field of artificial intelligence, is described as letting "computers learn without explicit programming. It teaches computers to learn by experience". ML in security continuously learns via data analysis, finding patterns and better detecting malware, find insider threats, and predicting potential unsafe areas online to protect those browsing. It also can protect data in the cloud by detecting suspicious user behaviors. CISCO, "What is ML in Security?" last accessed December 2, 2022.
[115] "Robotic process automation (RPA), also known as software robotics, uses automation technologies to mimic back-office tasks of human workers, such as extracting data, filling in forms, and moving files." It can "also access information through legacy systems, integrating well with other applications through front-end integrations. This allows the automation platform to behave similarly to a human worker, performing routine tasks, such as logging in and copying and pasting from one system to another." IBM Cloud Education, "RPA," *IBM*, October 22, 2020.
[116] IT Systems Expert Panel, *Essential Changes Imperative for the Success of Social Security's IT Modernization and Future Operations,* 22.

about the customer experience, performance management, design thinking, and a customer-focused strategy or blueprint.[117]

Multiple speakers presented themes that aligned with the Panel's CX recommendations for IT modernization. When discussing digital identity, speakers Lam and Hall highlighted the importance of improving service options and delivery according to user needs and preferences. Powner's presentation on cybersecurity addressed the importance of tying CX to the right outcome metrics for improved mission outcomes and emphasized the importance of CX for IT improvements. Cranor's presentation on Making Secure Systems Easy for the Public Use stresses the criticality of systems being both user-friendly and secure. Morton's entire session focused on CX, highlighting the VA's transformative focus on customer experience to inform agency change and service improvements.

The content in this expert series and the IT Panel's report provides important insights to inform agency IT modernization initiatives. The Board anticipates that this work will assist SSA in its ongoing modernization efforts and help the Congress and the administration in their oversight of SSA's IT modernization efforts.[118]

Bob Joondeph

Bob Joondeph,
Chair

Nancy J. Altman

Nancy J. Altman

Jagadeesh Gokhale

Jagadeesh Gokhale

[117] A complete listing of the Panel's customer experience recommendations are available here: IT Systems Expert Panel, *Essential Changes Imperative for the Success of Social Security's IT Modernization and Future Operations,* 23-25.

[118] Kim Hildred was a Board member through October 8, 2022, before the release of this report. Amy Shuart's appointment started on October 9, 2022, after the conclusion of the Systems Speaker Series.

Appendices

Glossary of Terms

Agile Software Development – a group of software development methodologies based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams.[119]

Artificial Intelligence – or AI, is a branch of computer science devoted to developing data processing systems that perform functions normally associated with human intelligence, such as reasoning, learning, and self-improvement. It is also the capability of a device to perform functions that are normally associated with human intelligence, such as reasoning, learning, and self-improvement.[120]

Assembly Language – also known as assembler language, a low-level programming language designed to communicate instructions with specific computer hardware and direct the flow of information.[121]

Attack Vector – a pathway or method used by a hacker to illegally access a network or computer in an attempt to exploit system vulnerabilities. Hackers use numerous attack vectors to launch attacks that take advantage of system weaknesses, cause a data breach, or steal login credentials.[122]

Authentication – verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.[123]

Authenticator Assurance Level – or AAL, is a measure of the strength of an authentication mechanism and, therefore, the confidence in it, as defined in

---

[119] CISCO, *Agile Product Development at CISCO: Collaborative, Customer-Centered Software Development*, White Paper, 2011.
[120] Department of Commerce (DOC), NIST, "AI," last accessed December 2, 2022. Also see: CISCO, "AI," last accessed September 28, 2022.
[121] Megha Thakkar, "What is Assembly Language? A Quick Overview," *InfoSec Insights by Sectigo Store*, May 3, 2022.
[122] Fortinet, "What is an Attack Vector," last accessed December 2, 2022.
[123] DOC, NIST, "Authentication," last accessed December 2, 2022.

[NIST SP 800-63-3[124]] in terms of three levels: AAL1 (Some confidence), AAL2 (High confidence), AAL3 (Very high confidence).[125]

Category Management – or CM, is a commercial best practice for buying common goods and services, to find the best value, meet the government's small business goals, and ultimately save money for taxpayers.[126]

Cloud – The cloud refers to servers that are accessed over the Internet and the software and databases that run on those servers. The cloud enables users to access the same files and applications from almost any device because the computing and storage takes place on servers in a data center, instead of locally on the user device. By using cloud computing, users and companies do not have to manage physical servers themselves or run software applications on their own machines.[127]

Common Business-Orientated Language (COBOL) – a high-level computer programming language first used in the 1960s and very popular in the business community. COBOL's popularity began declining in the 1990s, and it is now considered an outdated programming language, often the programming language (or code) of legacy systems. Although considered outdated, COBOL is still in use today.[128]

Commercial-Off-the-Shelf (COTS) – a software and/or hardware product that is commercially ready-made and available for sale, lease, or license to the general public.[129]

Common Services – common services purchased by GSA's FAS include training, overnight delivery services, copier machines, travel, and many IT solutions.[130]

---

[124] Paul A. Grassi, Michael E. Garcia, and James L. Fenton, *Digital Identity Guidelines*, DOC, NIST, Special Publication 800-63-3, June 2017.
[125] DOC, NIST, "AAL," last accessed December 2, 2022.
[126] Performance.gov, "CM: Leveraging Common Contracts and Best Practices to Drive Savings and Efficiencies," last accessed December 2, 2022.
[127] Cloudfare, "What is the Cloud?," last accessed December 2, 2022.
[128] For more information about COBOL see: Smithsonian, National Museum of American History, "COBOL," last accessed December 2, 2022; Patrick Stanard, "Today's Business Systems Run on COBOL," *TechChannel*, March 10, 2021.
[129] DOC, NIST, "COTS," last accessed December 2, 2022.
[130] Laura Stanton, *IT Category Management*, GSA, Office of IT Category, Presentation to SSAB, January 27, 2022

Common Services Provider – a federal organization that provides National Security System-Public Key Infrastructure (NSS-PKI) support to other federal organizations, academia, and industrial partners requiring classified NSS-PKI support but without their own self-managed infrastructures.[131]

Development and Operations (DevOps) – the combination of development (Dev) and operations (Ops) to unite people, process, and technology in application planning, development, delivery, and operations. DevOps lets formerly siloed roles like development, IT operations, quality engineering, and security coordinate and collaborate. Teams adopt DevOps culture, practices, and tools to increase confidence in the applications they build, respond better to customer needs, and achieve business goals faster. DevOps helps teams continually provide value to customers by producing better, more reliable products."[132]

Development, Security, and Operations (DevSecOps) – a process that automates the integration security at every phase of the software development lifecycle, from initial design through integration, testing, deployment, and software delivery (contrasted with past approaches where security was added on at the end of the development cycle, often by a separate security team).[133]

Digital Economy – the economic effects of online shopping, digital media, the sharing economy, and other e-commerce developments captured within GDP and other Bureau of Economic Analysis statistics.[134]

Digital Transformation – the process of completely replacing manual, traditional, and legacy ways of doing business with the latest digital alternatives across all aspects of business, not solely technology.[135]

Edge Computing – a form of computing that is done on-site or near a particular data source, minimizing the need for data to be processed in a remote data center, shifting computing resources from central data centers and clouds closer to devices.[136]

---

[131] DOC, NIST, "CSP," last accessed December 2, 2022.
[132] Microsoft, "What is DevOps?", August 2022. Last accessed December 2, 2022.
[133] IBM Cloud Education, "What is DevSecOps?" IBM, July 30, 2020.
[134] Bureau of Economic Analysis, "Special Topics," last accessed December 2, 2022.
[135] Hewlett Packard Enterprise, "Digital Transformation," last accessed December 2, 2022.
[136] Hewlett Packard Enterprise, "Edge Computing," last accessed December 2, 2022; CISCO, "What is Edge Computing," last accessed December 2, 2022.

Federal Information Security Modernization Act (FISMA) – FISMA requires federal agencies to implement a mandatory set of processes and system controls designed to ensure the confidentiality, integrity, and availability of system-related information. The processes and systems controls in each federal agency must follow established Federal Information Processing Standards, National Institute of Standards and Technology standards, and other legislative requirements pertaining to federal information systems, such as the Privacy Act of 1974.[137]

Federal Information Security Modernization Act (FISMA) of 2014 – Amends the Federal Information Security Management Act of 2002 (FISMA) to (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.[138]

Federal Risk and Management Program (FedRAMP) – a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP empowers agencies to use modern cloud technologies, with emphasis on the security and protection of federal information, and helps accelerate the adoption of secure, cloud solutions.[139]

IAL1 – NIST 800-63-3 identity assurance level 1 (IAL1)- a standard requiring evidence supporting real-world existence of the claimed identity, but has no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the subject's activities are self-asserted or should be treated as self-asserted, which are neither validated nor verified.[140]

IAL2 – NIST 800-63-3 identity assurance level 2 (IAL2)- a standard requiring evidence supporting the real-world existence of the claimed identity and verifies

[137] GSA, "FISMA," January 24, 2018.
[138] FISMA of 2014, Pub. L. no. 113-283 (December 18, 2014); For more information see: CISA, "FISMA," last accessed December 2, 2022.
[139] GSA's FedRAMP see: GSA, "FedRAMP," last accessed December 2, 2022.
[140] Department of Commerce (DOC), NIST, "Authentication," last accessed December 2, 2022.

that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically-present identity proofing.[141]

Journey Map – a visualization of the major interactions shaping a user's experience of a product or service. To provide design teams with a bird's-eye view of a service that helps them see the sequence of interactions that make up a user's experience including the complexity, successes, pain points, and emotions users experience from the earliest phases of researching a product or service - through adoption.[142]

Legacy System – an information system based on outdated technologies and critical to day-to-day operations. (Note: Replacing and modernizing legacy applications and systems with new and different technologies is a significant challenge. As organizations modernize their IT, they must ensure the new technology is compatible with older systems and data formats -until they can be fully modernized or replaced).[143]

Machine Learning – a domain within the larger field of artificial intelligence, is described as letting "computers learn without explicit programming. It teaches computers to learn by experience." ML in security continuously learns via data analysis, finding patterns and better detecting malware, find insider threats, and predicting potential unsafe areas online to protect those browsing. It also can protect data in the cloud by detecting suspicious user behaviors.[144]

Module – in A Module is any of a number of distinct but interrelated units from which a program may be built up or into which a complex activity may be analyzed.[145]

Multi-Factor Authentication – authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/personal identification number (PIN)); (ii) something you have (e.g.,

---

[141] For more information about NIST identity assurance levels see: Paul A. Grassi, Michael E. Garcia, and James L. Fenton, *Digital Identity Guidelines*, DOC, NIST, Special Publication 800-63-3, June 2017, last accessed September 28, 2022.
[142] GSA, 18F Methods, "Journey Mapping," last accessed December 2, 2022. Also see Performance.gov, "Mapping the Cros-Agency CX," January 28, 2021.
[143] Sygma Technology, "What are Legacy Systems," last accessed December 2, 2022.
[144] CISCO, "What is ML in Security?" last accessed December 2, 2022.
[145] Testapedia, "Module," last accessed December 2, 2022.

cryptographic identification device, token); or (iii) something you are (e.g., biometric).[146]

NIST 800-63-3 – National Institute of Standards and Technology Special Publication 800-63-3 Digital Identity Guidelines provide technical requirements for federal agencies implementing digital identity services. They cover identity proofing and authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks and technical requirements in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions.[147]

Personally Identifiable Information – or PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.[148]

Real-Time – real-time pertains to the performance of a computation during the actual time that the related physical process transpires so that the results of the computation can be used to guide the physical process.[149]

Robotic process automation – or RPA, also known as software robotics, uses automation technologies to mimic back-office tasks of human workers, such as extracting data, filling in forms, and moving files. It can also access information through legacy systems, integrating well with other applications through front-end integrations. This allows the automation platform to behave similarly to a human worker, performing routine tasks, such as logging in and copying and pasting from one system to another.[150]

Security Platforms – security platforms integrate vendor-specific and third-party functions, allowing security teams to work more efficiently, faster, and

---

[146] DOC, NIST, "MFA," last accessed December 2, 2022.
[147] Paul A. Grassi, Michael E. Garcia, and James L. Fenton, *Digital Identity Guidelines*, DOC, NIST, Special Publication 800-63-3, June 2017, last accessed December 2, 2022.
[148] DOC, NIST, "PII," last accessed December 2, 2022.
[149] DOC, NIST, "Real-Time," last accessed December 2, 2022.
[150] IBM Cloud Education, "RPA," *IBM*, October 22, 2020.

more collaboratively by simplifying integration, improving visibility, sharing intelligence, and automating workflows across endpoints, cloud, network, and applications.[151]

Technical Debt – (also known as "tech debt" or "code debt") implies costs from choosing an easy (or limited) IT solution now - instead of using a better, longer-term solution. There is a tradeoff between the short-term benefits of rapid delivery and the long-term value of developing a software system that is easy to evolve, modify, repair, and sustain. Like financial debt, technical debt can be a burden or an investment.[152]

Verification – the process of confirming or denying that a claimed identity is correct by comparing the credentials of a person requesting access with those previously proven and associated with the PIV Card or a derived PIV credential associated with the identity being claimed.[153]

Zero Trust – a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgment that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information fed from multiple sources to determine access and other system responses.[154]

---

[151] CISCO, "What is a Security Platform," last accessed December 2, 2022.
[152] Splunk, "What is Tech Debt," last accessed December 2, 2022; Carnegie Mellon University, Software Engineering Institute, "Managing Technical Debt with Data-Driven Analysis," February 2022.
[153] DOC, NIST, "Verification," last accessed December 2, 2022.
[154] NSA, Embracing a ZT Security Model, February 2021.

Speaker Series Expert Presenter Bios

Renato (Renny) DiPentima – Historical Overview of Social Security's IT Systems

Renato ("Renny") A. DiPentima, PhD serves on the Boards of Directors of Cap Gemini Government Solutions, Amida Technology Solutions, iNovex Information Systems, and Gunnison Consulting Group, as well as the Advisory Board at Blue Delta Capital Partners. DiPentima also served as a board director for Brocade Communication Systems. DiPentima held several senior management positions in the federal government, including serving as Social Security Administration's deputy commissioner and as the agency's CIO and also served on the Board's IT Systems Expert Panel.

Alan Balutis – Historical Overview of Social Security's IT Systems

Alan Balutis, PhD is a former distinguished fellow and senior director of North American Public Sector Cisco Systems' Business Solutions Group, the firm's global strategy, and consulting arm. Balutis served more than 30 years in public service and industry leadership roles and is a founding member of the Federal Chief Information Officers (CIO) Council. As a founding member, he led its strategic planning and outreach committees, helped create the council's e-government committee, and served as its first chair. At the Department of Commerce, Balutis headed the management and budget office for over a decade and was the department's first CIO. Balutis won the Federal Computer Week FED 100 eight times and is a member of the Government Computer News and the Federal Computer Week halls of fame. He is also a fellow of the National Academy of Public Administration (NAPA) and chaired the Board's IT Systems Expert Panel.

Phil Lam – Digital Identity

Phil Lam is the Executive Director of Identity at the Technology Transformation Service in the General Services Administration (GSA). As GSA's lead on identity, Lam implements and promotes identity as a shared service across government to improve constituent access to government services. Lam's past work includes creating and implementing an industry-level strategy for digital identity. Lam earned a BS in Computer Engineering from Northwestern University and an MBA in Management Analytics from Purdue University.

Blake Hall – Digital Identity

Blake Hall is the Founder and CEO of ID.me, the next-generation digital identity network that simplifies how individuals securely prove their identity online. Consumers can verify their identity with ID.me once and seamlessly prove their identity to over 500 organizations without needing to re-verify identity. Government agencies, healthcare organizations, financial institutions, and consumer brands use ID.me to verify customer identity. In 2019, Hall was named CEO of the Year by One World Identity. Prior to ID.me, Hall led a reconnaissance platoon in Iraq and was awarded the Bronze Star with Valor for stopping an Al-Qaida assault on a Combat Support Hospital in Mosul, Iraq. Hall won a second Bronze Star for exceptional performance hunting high value targets and holds a BS magna cum laude from Vanderbilt University and an MBA from Harvard Business School.

Kevin C. Walsh – Modernizing Legacy IT Systems

Kevin C. Walsh is the Director of Information Technology (IT) and Cybersecurity at the Government Accountability Office (GAO). Walsh oversees work related to Chief Information Officer (CIO) authorities, Department of Homeland Security and Department of Defense systems, legacy modernizations, satellite and space systems, coordination of IT contracts, and assessments of IT-related risk. Walsh joined GAO in June 2006 and earned an MBA from Virginia Tech and a bachelor's degree in economics from the University of Maryland, College Park.

Robert Klopp – Modernizing Legacy IT Systems

Robert Klopp is the Owner/Principal Consultant of Skyland Digital Services, Inc. Klopp previously was a Presidential appointee and served as Social Security's Deputy Commissioner, CIO, and Chief Technology Officer, managing a budget of $1.2 billion. Klopp's achievements at Social Security included establishing a modern cloud platform strategy and an agile customer-oriented development methodology. Klopp also implemented software engineering best practices across the agency.

Barbara C. Morton – Customer Experience as a Driver for IT Modernization

Barbara C. Morton has served as the Deputy Chief Veterans Experience Officer since 2016. In this role, Morton is responsible for building a lasting customer experience capability at the Department of Veterans Affairs (VA) and sharing best practices across federal agencies. Previously, Morton briefly served as the

Acting Chief Veterans Experience Officer. Morton was recently an agency recipient for the Gears of Government Award (2019) and the Service to the Citizen Award (2019) for transforming the VA capability to provide veterans with an excellent customer experience. Morton joined the VA in 2006 as a Staff Attorney at the Board of Veterans' Appeals. Morton served in a variety of related capacities, including Special Counsel to the Appellate Group, Special Assistant to the Vice Chairman, Executive Assistant to the Chairman, and Executive Director for the Office of Management, Planning & Analysis. At the Board of Veterans' Appeals, Morton also helped secure industry technologists from United States Digital Service to develop and launch new appeals platforms. Morton holds a degree in psychology and philosophy from Skidmore College, a JD from Suffolk University Law School, and an LLM in constitutional law from Georgetown Law School.

Dave Powner – Federal Cybersecurity Landscape

Dave Powner is the Executive Director of the Center for Data-Driven Policy and the Director of Strategic Engagement and Partnerships at the MITRE Corporation. In this role, he enhances MITRE's strategic corporate partnership interactions and development of new opportunities with the federal government, states, the private sector, and academia. Powner has more than 25 years of experience in both the public and private sectors. Before joining MITRE, Powner served as a Director at the Government Accountability Office where he led numerous reviews of federal information technology that resulted in testifying before Congress more than 100 times. During his tenure, Powner played a key role in the implementation of the Federal Information Technology Acquisition Reform Act (FITARA), led the creation of the FITARA Scorecard, and contributed his expertise to the development of the Modernization Government Technology Act. Powner is a Fellow at the National Academy of Public Administration and a Strategic Advisor to Government Executives at the Partnership for Public Service. He has won numerous Federal Computer Week's Federal 100 awards and was the federal government's top awardee of the Eagle award in 2017 for his contributions to the federal information technology community. Powner holds a bachelor's degree in business administration from the University of Denver and completed the Senior Executive Fellows program at the Harvard Kennedy School.

Jim Richberg – Federal Cybersecurity Landscape

Jim Richberg is the Public Sector Field CISO and Vice President of Information Security at Fortinet. He has over 30 years of experience leading and driving innovation in cybersecurity, threat intelligence, cyber strategy and policy for the US government and international partners. Prior to joining Fortinet, Richberg served as the National Intelligence Manager for Cyber, the senior federal executive focused on cyber intelligence within the intelligence community. Richberg led the creation and implementation of cyber strategy for 17 intelligence departments and agencies, set integrated priorities on cyber threat, and served as Senior Advisor to the Director of National Intelligence on cyber issues. Richberg created and oversaw implementation of the multi-billion dollar whole-of-government Comprehensive National Cybersecurity Initiative that generated new government cyber capability and enhanced cybersecurity in the private sector and critical infrastructure. Richberg gained practical insight into advanced threat capabilities, insider threat, and supply chain integrity during his 20 years at the CIA. Richberg helped build the discipline of cyber threat intelligence analysis and has been an innovator in measuring cyber performance, risk, and return on investment. Richberg holds a BA in political science from Ohio University and a master's degree in international relations from Stanford University.

Laura Stanton – IT Acquisition

Laura Stanton is the Assistant Commissioner for the Office of Information Technology Category (ITC) in GSA's Federal Acquisition Service (FAS). The FAS provides buying platforms and acquisition services to Federal, DoD, State, and Local governments for a broad range of items, from office supplies and motor vehicles to information technology and telecommunications products and services. As an organization within FAS, ITC provides access to a wide range of commercial and custom IT products, services, and solutions. As Assistant Commissioner, Laura manages the largest fee-for-service IT procurement and services operation in the US government. Laura leads a highly-skilled and diverse workforce that manages more than 6,000 contracts, providing access to relevant and timely IT and telecommunications products, services, and solutions to defense and civilian agencies, as well as to state, local, and tribal governments. ITC facilitates more than $32 billion in annual government spending and has provided nearly $2 billion in savings to its customers. Before rising to lead ITC, Laura served as its Deputy Assistant Commissioner for Category Management, where she oversaw a portfolio of acquisition solutions, including the Government-wide Acquisition Contracts (GWACs) Alliant 2, VETS 2, and 8(a) STARS II. In addition, her portfolio also included the Enterprise

Infrastructure Solutions (EIS) and the USAccess shared services programs. Laura's guidance and oversight of the category teams helped ITC play a critical role in the Administration's IT modernization efforts to drive a more efficient and effective government for the American people. Laura came to ITC from GSA's Office of Enterprise Strategy Management. As the Assistant Commissioner, Laura directed FAS's strategic business planning, performance management, category management, and Acquisition Gateway adoption. She played an integral role in creating and executing a FAS strategic vision that aims to establish itself as the Government Acquisition Marketplace. She also coordinated with the Category Management Leadership Council and the Office of the Federal Procurement Policy to implement category management government-wide. Laura was named a recipient of the 2015 Federal 100 Awards, presented to government, industry, and academic leaders who have played pivotal roles affecting how the federal government acquires, develops, and manages IT. Laura received her BA from Smith College and an MPP from Georgetown University. Her thesis on broadband adoption was published by the IEEE, the world's largest professional association for the advancement of technology.

Bill Zielinski – IT Acquisition

Bill Zielinski has served as the Chief Information Officer (CIO) for the City of Dallas since June 2020. Previously, Zielinski was the Assistant Commissioner for ITC in GSA's FAS. Before that, Zielinski provided oversight of the federal government's IT capital planning and investment control process for the Federal CIO. Additionally, he served as the CIO for the Social Security Administration (SSA) between 2013 and 2015, where he led a staff of approximately 3,400 IT Specialists and managed an annual total budget of more than $1.5 billion. Prior to being the CIO, Zielinski served as the Regional Commissioner for SSA's San Francisco Region. Zielinski received a BS from Washington State University.

Lorrie Cranor – Making Secure Systems Easy for the Public to Use

Lorrie Cranor is the Director and Bosch Distinguished Professor in Security and Privacy Technologies of CyLab and the FORE Systems Professor of Computer Science and of Engineering and Public Policy at Carnegie Mellon University. She is also co-director of the Collaboratory Against Hate: Research and Action Center at Carnegie Mellon and the University of Pittsburgh. She directs the CyLab Usable Privacy and Security Laboratory (CUPS) and codirects

the MSIT-Privacy Engineering masters program. In 2016 she served as Chief Technologist at the Federal Trade Commission and is also a co-founder of Wombat Security Technologies, a security awareness training company acquired by Proofpoint. She has authored over 200 research papers on online privacy, usable security, and other topics. She has played a key role in building the usable privacy and security research community, having co-edited Security and Usability (O'Reilly 2005); founded the Symposium on Usable Privacy and Security (SOUPS); co-founded the Conference on Privacy Engineering Practice and Respect (PEPR); chaired the Platform for Privacy Preferences Project (P3P) Specification Working Group at the W3C; and authored Web Privacy with P3P (O'Reilly 2002). She has served on the Board of Directors for the Electronic Frontier Foundation and the Computing Research Association, and on the editorial boards of several journals. More recently she named an ACM, IEEE, and AAAS Fellow. She is also a 2019 Andrew Carnegie Fellow and has received an Alumni Achievement Award from the McKelvey School of Engineering at Washington University in St. Louis, the 2018 ACM CHI Social Impact Award, the 2018 International Association of Privacy Professionals Privacy Leadership Award, and (with colleagues) the 2018 IEEE Cybersecurity Award for Practice. She was previously a researcher at AT&T-Labs Research and taught in the Stern School of Business at New York University. She holds a doctorate in Engineering and Policy from Washington University in St. Louis.

Acknowledgments

Former Board Member Kim Hildred (2016-2022) contributed significantly to the Board's work on IT Modernization, including the Board's IT Systems Expert Panel and the subsequent IT Systems Speaker Series. We thank Kim Hildred for her service to the Board and her efforts culminating in this paper.

The Board is grateful to all those who shared their knowledge and expertise to inform this work. First and foremost, a very special thank you to the experts who took their time to prepare and present, including Renny DiPentima, Alan P. Balutis, Phil Lam, Blake Hall, Kevin C. Walsh, Robert Klopp, Barbara C. Morton, Dave Powner, Jim Richberg, Laura Stanton, Bill Zielinski, and Lorrie Cranor.

Staff contributors to this report include Pamela Crawford (Senior Advisor), Diane Brandt (Research Director), and Claire Green (Staff Director). Additional staff supported the speaker series events, including Emma Tatem (Lead Policy Analyst), Conway Reinders (Lead Policy Analyst and Communications Officer), and Omar Shalabi (Policy Analyst).

About the Board

The Social Security Advisory Board is a bipartisan, independent federal agency established in 1994 to advise the President, Congress, and Commissioner of Social Security on matters of policy and administration of the Old-Age, Survivors, and Disability Insurance and Supplemental Security Income programs. The Board has seven members, appointed by the President, Senate, and House of Representatives.

Social Security Advisory Board
400 Virginia Avenue SW, Suite 625
Washington, DC 20024

@ssabgov www.ssab.gov