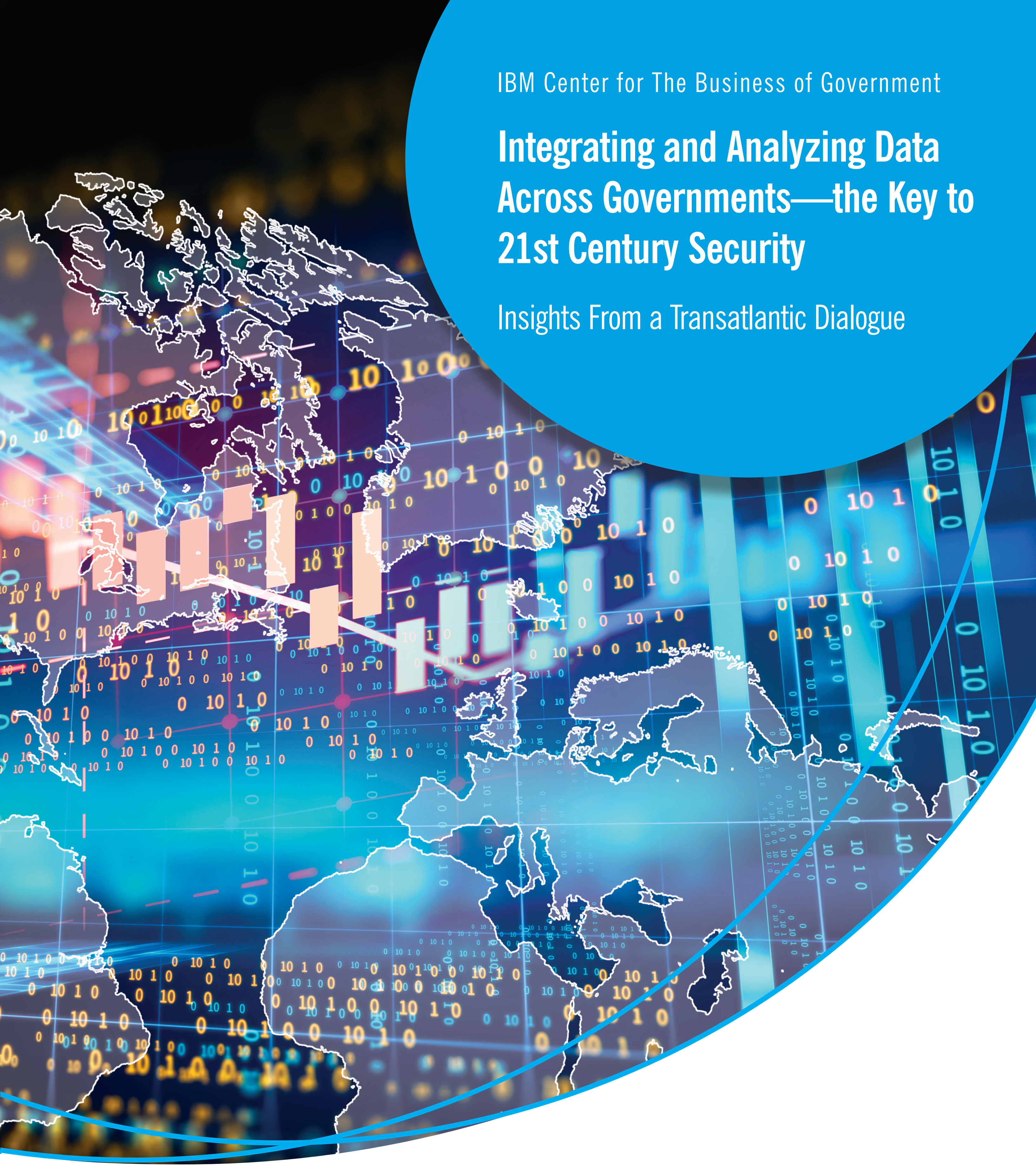
IBM Center for The Business of Government

Integrating and Analyzing Data Across Governments—the Key to 21st Century Security

Insights From a Transatlantic Dialogue



Douglas Lute

Senior Fellow, Harvard Belfer Center for Science and International Affairs

Francis Taylor

Executive Fellow, Keough School of Global Affairs, University of Notre Dame

IBM Center for
The Business of Government
20 years of research for government:
informing today, envisioning tomorrow
1998-2018

Integrating and Analyzing Data Across Governments—the Key to 21st Century Security

2018

Insights From a Transatlantic Dialogue

Douglas Lute
Senior Fellow, Harvard Belfer Center for Science
and International Affairs

Francis Taylor
Executive Fellow, Keough School of Global Affairs
University of Notre Dame

1998-2018
IBM Center for
The Business of Government
20 years of research for government:
informing today, envisioning tomorrow

TABLE OF CONTENTS

FOREWORD

On behalf of the IBM Center for The Business of Government, we are pleased to present this special report, *Integrating and Analyzing Data Across Governments—the Key to 21st Century Security,* by Douglas Lute (LTG, Ret.), Senior Fellow with the Harvard University Belfer Center for Science and International Affairs and former U.S. Ambassador to NATO, and Francis Taylor (BG, Ret.), Executive Fellow with the Notre Dame Keough School of Global Affairs and former Undersecretary for Intelligence and Analysis with the U.S. Department of Homeland Security.

This report focuses on data gathering, analysis, and dissemination challenges and opportunities across the homeland security enterprise, looking especially at how improved information sharing could enhance threat prediction and prevention in a transatlantic context. The authors address how stakeholders in the U.S. and Europe can increase the understanding of effective ways to leverage channels involving technology, human capital, organizations, and private sector coordination that meet strategic, mission, and operational needs. The report highlights opportunities for governments to leverage data integration and analytics to support better decision making around cyber and homeland security.

The authors draw primarily on findings from two roundtable discussions with current and former government leaders and stakeholders. The first meeting, held in Washington, D.C. in October 2017, focused on how the U.S. Department of Homeland Security (DHS) information sharing enterprise can have the greatest impact and interaction with partners. The second meeting, held at the U.S. Mission to the European Union (EU) in Brussels in March 2018, focused on how the European Union and other European organizations and member states can work with U.S. agencies to enhance outcomes from improved information sharing.

Given the imperative for transatlantic and cross-sector collaboration to understand and respond to an increasingly complex set of threats facing governments, we hope that this report provides timely insights for public sector leaders and stakeholders.

DANIEL J. CHENOK

LEENDERT VAN BOCHOVEN

Daniel J. Chenok
Executive Director
IBM Center for The Business of Government
chenokd@us.ibm.com

Leendert Van Bochoven
Global Lead, Defense & Intelligence
IBM Global Government
L_van_Bochoven@nl.ibm.com

DONALD FENHAGEN

Donald Fenhagen
Partner, Department of Homeland Security
IBM Global Business Services
fenhagen@us.ibm.com

INTRODUCTION

The IBM Center for The Business of Government recently hosted two roundtable discussions with current and former government leaders and stakeholders, focused on integrating and analyzing data within and across governments on both sides of the Atlantic to improve threat prediction and prevention.

The first meeting, in October 2017, addressed how the U.S. Department of Homeland Security (DHS) information sharing enterprise can have the greatest impact and interaction with partners. The second meeting, in March 2018, addressed how the European Union (EU) and other European organizations and member states can work with DHS, the Department of State, and other U.S. agencies, to best enable a trusted environment for sharing information. These sessions were conducted under non-attribution, Chatham House rules; see Appendix for a list of Roundtable participants.

Two major themes from these robust discussions were identified. The first revolved around data requirements, gathering, analysis, and dissemination challenges across the homeland security enterprise. The second theme identified how addressing these challenges will help DHS, the EU, and related stakeholders understand common operational needs and strengthen transatlantic information sharing and collaboration, especially in light of EU protections for privacy and data security. Other topics included how best to assist DHS and other stakeholders in using information to achieve strategic and mission outcomes, the expertise within government needed to develop and maintain solutions, and external linkages needed to ensure successful implementation.

U.S. and EU organizations can learn from each other’s experiences. Both discussions found that solutions were not predominantly technology-focused, but rooted in human-based institutions along with deficits in trust. Specifically, mutual learning can advance in several areas, including:

- **Fostering cross-domain or cross-function approaches to government data**—U.S. agencies are developing policies, processes, and technology to resolve these issues, and the U.S. government has made data strategy a new cross-agency priority goal.

- **Analytics through a rules-based approach,** instead of binary calculation. DHS has made progress in this arena.
- **Industry partnerships.** For example, the U.S. government has developed numerous public-private partnerships to address cyber information sharing.
- **Information sharing across multilateral collaboratives,** like the Schengen Area, which is the integrating factor across Europe. Schengen is a region of 26 European countries that do not require a passport or other controls to cross their borders.
- **The process of developing and implementing the General Data Protection Regulation (GDPR) legislation and similar policies,** which have enabled the EU to promote a much more robust debate about the relationship between government and citizens involving data protection.

This report addresses key challenges and opportunities raised by participants in the two roundtables. The report is divided into four sections, each of which identifies experiences and options to foster more effective information sharing across borders:

- Trust in Data: A Human Challenge for Both the U.S. and EU
- How Analytics Can Improve Information Sharing
- Bureaucratic Considerations
- The Role of Private Sector Partners

The report concludes with a review of key lessons to be shared among nations and stakeholders regarding how best to move forward in this critical area of governance.

Trust in Data: A Human Challenge for Both the U.S. and EU

Sharing data more effectively across governments and organizations is a key to effective democracy. However, this can only happen in a climate of trust among governments and with companies and citizens. Building citizen trust in and across agencies is imperative. Citizens may not realize that sharing information improves the government's ability to prevent attacks. Agencies can promote citizen confidence by implementing data access rights, ensuring transparency, and demonstrating and communicating the benefits of data sharing that respects privacy and security rules in terms of reduced burden and cost. For example, trust might be built by government's communicating effectiveness in sharing less sensitive data to promote efficiency and convenience for the provider, such as sharing driver's license data across states before attempting to share health data. By using data responsibly, and communicating that use to citizens, industry, and government partners, agencies can build trust in data handling and support for data sharing.

Two key factors emerge in building trust in data across governments and with data providers: security that demonstrates data will be shared based on known parameters, limited as agreed by providers of the information, and controlled based on good technical practice; and integrity that demonstrates data will not be compromised, manipulated or altered. At the same time, deficits in trust about data integrity often exist between providers and end-users. Both government and commercial organizations work with multiple information sharing networks, some of which lie dormant, or are underutilized due to a lack of trusted relationships with intended end-users. Successful sharing relationships typically allow a degree of ownership by end-user coalitions such that information by agency leaders is shared "top down," and by practitioners is shared "bottom up."

Moreover, inadequate data sharing and trust present a national security concern for the U.S. and EU member states. Individuals about whom derogatory data exists but who are not actively monitored can execute attacks. If countries can aggregate, share, and analyze data collected in real time, and transmit that data to those who need it, the threat picture would become much clearer and allow for earlier, decisive action.

The U.S. and EU must collaborate to incentivize collective action that builds trust, both domestically and across borders. A human challenge exists with information sharing and data integration for national and international security concerns. This human challenge impacts institutional trust among information owners. Various examples of progress can provide a path forward toward enhanced trust.

Case Studies in the U.S. and EU

The U.S. faces institutional trust issues among different levels of government. Federal, state, and local agencies have a myriad of perspectives about the process for information sharing. Against this backdrop, DHS has made great strides in scaling collaboration.

The Homeland Security Information Network (HSIN) was created as an extension of the Joint Regional Information Exchange System (JRIES), first piloted in 2002. In 2003, JRIES was renamed as HSIN and transferred from the Defense Intelligence Agency (DIA) to DHS.[1] HSIN is the trusted network for homeland security mission operations to share sensitive but unclassified information.[2] Federal, state, local, territorial, tribal, international, and private sector homeland security partners use HSIN to manage operations, analyze data, send alerts and notices, and generally share information they need to do their jobs. Today, HSIN has approximately 100,000 users that cross federal, state, local, and tribal networks.

[1] https://www.oig.dhs.gov/assets/Mgmt/OIG_06-38_Jun06.pdf

[2] https://www.dhs.gov/what-hsin

A high-profile case when HSIN successfully shared information across networks involved the Boston Marathon Bombing in 2013. After that tragic event, HSIN shared information that enabled analysis of multiple inquiries from the Boston area to assess conditions on the ground and determine if the incident extended beyond Boston.

At the same time, DHS faces a current HSIN challenge of scaling human collaboration. HSIN is an automated experience, and does not in and of itself support high-level face-to-face interactions that result in building trust. A variety of approaches may add this interpersonal element. Virtual collaborations, conferences, training, and other face-to-face meetings can play an important part in human interactions and networks. As people move to different organizations and new roles, creating a network of intelligence professionals through face-to-face meetings can improve and maintain trust among partners on HSIN.

HSIN, along with the National Information Exchange Model (NIEM), is a model for how common standards for data sharing allow public and private enterprises to operate under similar understandings, which is important to ensuring that stakeholder groups trust one another. This can promote data integration and bridge cultural divides across borders.

The EU faces similar successes and challenges with information sharing. The EU created Europol (the European Agency for Law Enforcement Cooperation)[3] in 1998 to coordinate law enforcement actions, which connected stakeholders from many EU member states. Europol's decentralized information sharing system is voluntary for EU member states. In 2015, the Europol information sharing system had 1.5 million hits, and a year later the system had 2 million hits. As the system shows value, user networks grow rapidly as they derive value from the data.

The EU also uses the Secure Information Exchange Network Application (SIENA),[4] an encrypted tool hosted by Europol that allows for biometric data and the dissemination of information across the EU. SIENA provides 24/7 communication among agencies. But while automation allows agencies to operate with less human interaction, the human element still exists. People from different agencies still need to be in direct contact to organize meetings, work with the system to code data sharing routines, troubleshoot system issues, configure the system to automate the appropriate tasks, and continuously gain user feedback to make improvements to the application.

Apart from the successes of HSIN and Europol's information sharing system, more work remains to measure success in information sharing and build institutional trust among levels of government in the U.S. and the EU. Efforts to increase collaboration, promote collaborative innovation regarding intelligence and response, and increase transparency of information lead to more trust. A system to ensure the chain of data custody and help organizations comply with important policies will lead citizens to be more comfortable sharing their data.

By leveraging relationships, agencies can improve value and confidence in information sharing while not duplicating work. One model would involve allowing the information creator to maintain control, while enabling information to be disseminated among the community—perhaps through a standard query system that helps identify common data stores. Technologies such as blockchain could potentially add value to the information sharing network; blockchain could add an additional layer of security and transparency to data flows that cannot be altered.

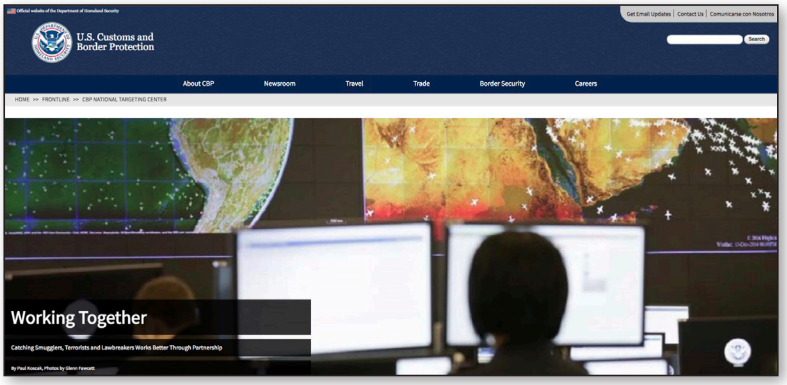
[3] https://www.Europol.europa.eu

[4] https://www.Europol.europa.eu/activities-services/services-support/information-exchange/secure-information-exchange-network-application-siena

Augmenting Human Capabilities with Technology and Measuring Success

When measuring success, DHS faces issues with systemic sharing across small communities. The challenge lies with connecting some 800 communities as part of a secure information sharing network, and increasing the impact of community-to-community sharing. Interoperable and infrastructure platforms that leverage cloud computing in a secure manner will provide a foundation for rapid sharing and analytics. Such connectivity can enhance trust.

Technology can support improved sharing of information. A few examples show how technology augments human capabilities to analyze data in a quicker and more efficient way. The U.S. Customs and Border Protection (CBP) created the National Targeting Center[5] after 9/11. Analysts looked at the available data and identified risks of goods coming into the country. This brought together staff from the U.S. Postal Service, the Food and Drug Administration, and other relevant partner agencies. Each organization added data about certain carriers into the targeting center, which enabled risk scoring about countries importing goods into the U.S. This risk score substantially helped CBP decide if they needed to act on information, which made their response more efficient. In addition, the National Targeting Center has evolved to include analysis of information on threats posted by travelers to the U.S.


Official website of the Department of Homeland Security
Get Email Updates | Contact Us | Comunicarse con Nosotros
U.S. Customs and Border Protection
Search
About CBP
Newsroom
Travel
Trade
Border Security
Careers
HOME >> FRONTLINE >> CBP NATIONAL TARGETING CENTER

Working Together

Catching Smugglers, Terrorists and Lawbreakers Works Better Through Partnership

By Paul Koscak, Photos by Glenn Fawcett

Source: Department of Homeland Security. National Targeting Center.

Current human queries can be made more efficient if augmented by an automated information sharing system. Fusion cells are an example of where technology can enhance the human element for information sharing effectiveness and connect stovepipes across government. For example, the U.S. Department of Defense's (DoD) Joint Operations Center[6] faced the urgent problem to defeat Al Qaeda in Iraq. An interagency fusion cell was created and key agencies were co-located to share information and strategize. Over time, this human connection broke through what had been stovepiped information channels. Proximity is key and co-locating people to simply talk to one another in person is a critical step in advancing information sharing across agencies. Fusion cells can connect the right people with the right clearances and provide access to key data, while technology can facilitate sharing at speed and scale.

Programs like this can foster the development of a new culture to increase trust and information sharing. The new culture should incentivize data sharing through performance metrics,

[5] https://www.cbp.gov/frontline/cbp-national-targeting-center

[6] https://www.army.mil/article/180736/combined_joint_operations_center_baghdad_brings_coalition_together_for_operation_inherent_resolve

standards, and mutual knowledge to break cultural divides. That said, the “human element” might be harder to crack as operators become concerned that automation will change their job and processes. Some operational line staff believe that automation will put them out of work. They fear that automation will focus performance evaluation on metrics that emphasize quantity and speed over quality of analysis. However, automation can streamline workloads and allow operators to focus on mission achievement. To cross this bridge, government could start to facilitate culture change by proposing new performance metrics that have a positive effect on employees leveraging automated data sharing methods. Through automation, operators can capitalize on better and more mission focused outcomes from their analysis, to focus on what they do best. Automation also allows more data to be shared at speed and scale with partner organizations.

To leverage the promise of automation, agencies need to close a digital knowledge gap among policy makers, analysts, and data owners. More individuals should increase what one roundtable participant called their “digital IQ”—the skills to use emerging technologies, such as artificial intelligence (AI), and understand the foundations of data sharing and interoperability. A strong digital IQ can help government capacity keep pace with commercial innovation. IT training can enhance that understanding. For instance, proper training can ensure that individuals fully utilize technology across the global security community. Likewise, policy makers can better understand technology’s positive impact on information sharing. In both instances, agencies can make a stronger business case to fund modernized IT systems. In addition, policy makers can help citizens use technology responsibly, while ensuring that data exchange will benefit citizens through increased global security.

How Analytics Can Improve Information Sharing

Lack of interoperability and data integrity across existing information sharing platforms, and the largely disconnected and decentralized nature of data across governments, negatively affect the ability to assess trends and conduct deep, real-time, and predictive analysis. Data integrity is a dependency for sharing. Building analytics programs based on automated and auditable review of and appropriate responses to anomalies will promote integrity.

Leveraging new analytics technologies, including AI and blockchain platforms, can promote data integrity and interoperability that complies with appropriate standards while also improving the speed to turn raw data into actionable intelligence. The U.S. and EU share similar desires to advance their ability in sharing, analyzing, and responding to data in the national security space. There is a need for an effective, collaborative solution. Analytics can improve threat information sharing and collaboration across the U.S. and EU.

Governments can leverage analytics to translate data for wider audiences who assess information, create business intelligence, integrate results with additional data sources, and use rapid and secure information channels to send actionable information back out to front-line operators. Analytics technologies can replace large volumes of basic queries with data-driven information sharing systems, allowing authorities to collaborate and engage in higher order analysis and interpretation. But while AI and other emerging analytics technologies have a future in government and law enforcement, successful implementation relies on confidence in the security and accuracy of such technologies. HSIN offers a model for the value of such confidence. For technology to enable effective threat information sharing and collaboration across the U.S. and EU, governments must work together in protecting national interests given global threat vectors.

Innovations like new “5G” wireless systems, the Internet of Things (IOT), advanced encryption, and quantum computing make strict privacy protections essential. However, data security and privacy solutions, such as anonymization of data and secure identity management, can require significant resources and mature data protection systems. Since privacy and security are non-negotiable when dealing with sensitive information, especially with the full implementation of the General Data Protection Regulation (GDPR)[7] and the Directive on Security of Network and Information Systems,[8] the U.S. and EU face a choice. Governments can limit information sharing and collaboration to reduce privacy and security risks, or invest in technology that builds protective protocols into the sharing process. Leveraging AI and machine learning can ensure appropriate and secure access to databases by analysts working across systems and around the world.

[7] https://www.eugdpr.org

[8] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

Bureaucratic Considerations

Bureaucratic and structural challenges affect the management and development of the information sharing enterprise. Recent EU policies call for greater transparency and centralization of information, alongside the context of recent responses to terrorist incidents. Former DHS leaders have observed that the agency has all the information needed to carry out the homeland security mission, but that DHS components have not prioritized sharing sufficiently. The establishment of a National Intelligence Manager (NIM) for the Western Hemisphere and the homeland is a step to build on. In addition, in an effort to further harmonize and effectively share data, DHS established a National Vetting Center (NVC). The NVC will not have any additional collection authorities; however, it will focus on further sharing and synthesizing already collected material within the U.S. government.

Overcoming bureaucratic hurdles should not wait for a crisis. Governments should evaluate lessons learned from past events and take a longer view of how best to organize for effective sharing. In the past, it has taken national catastrophes to deliver top-down change for the U.S. This occurred with the change in DoD that emerged after the Vietnam War from a top-down act of Congress: the Goldwater-Nichols Act of 1986[9] reworked the command structure of the US military. This statute streamlined communication channels after the issues that contributed to the failure of the Iranian hostage rescue mission in 1980. Goldwater-Nichols reorganized DoD to account for the failures in Vietnam, including the stovepiping of the war effort among the four military services. It also created the separate, joint Special Operations Command to bring together specialists from across the services and promote unity after the hostage mission. Similarly, after the attacks on 9/11, organizational change included the creation of DHS and the Directorate of National Intelligence (DNI) to integrate fragmented elements of our national security structure. The U.S. Congress could similarly reevaluate their oversight of DHS given the myriad of committees and subcommittees with jurisdiction over the agency, the streamlining of which would further promote organizational agility and efficient use of resources by DHS in executing its mission.

Longer-term change can also result from bottom-up conversations among practitioners—both approaches can be integrated for effective reform. Governments should learn from these kinds of examples to promote bureaucratic effectiveness and to mitigate the disruptive changes that may result from an inadequate response to future national catastrophes due to bureaucratic challenges.

Cross-government memoranda of understandings (MOUs) can drive collective action for information sharing. For example, an initiative in Europe involving interagency collaboration has been introduced through a new system—the European Travel Information and Authorization System (ETIAS)[10]—enabling searchable sharing across multiple organizations, connecting existing databases, and supporting future related efforts. These organizations are currently collaborating on a border management database, which aims to provide authorization to travel to the EU for visa-exempt third-country nationals, and to prevent possible threats from entering the EU member states. Three organizational platforms are involved that will increase collective action:

- eu-LISA, the EU agency for the operational management of large-scale IT systems, will build a secure threat data platform and watch list;
- Frontex, the EU Border and Coast Guard Agency, will manage the ETIAS Central Unit and will be responsible for data quality assurance, definition, and implementation of risk indicators within the screening rules, as well as verifying travel authorization applications in cases of a hit obtained during the automated processing; and

[9] https://en.wikipedia.org/wiki/Goldwater%E2%80%93Nichols_Act

[10] https://www.schengenvisainfo.com/etias/

- Europol will manage the shared watch list, including updates via checking with INTERPOL databases in parallel.

Standardizing Rules and Translating Data into Action

When addressing inefficiencies, and trying to fix them in government, the natural tendency is to create one-off processes that inherently increase bureaucracy rather than fixing underlying inefficiencies. This trend happens time and again in the public sector. The EU faces the additional challenge of a lack of common data sharing agreements among member states. Navigating this complex terrain calls for simplifying the information sharing landscape, not more bureaucratic structure.

Technology can enable governments to standardize rules among layers of bureaucracy. Across U.S. defense and intelligence agencies, for example, different offices have different rules for collecting and storing information. Through rules-based automation, agencies can pull data in a manner that complies with appropriate processes and makes information sharing faster within law and policy constraints. In addition, support for information sharing among agencies may emerge more naturally if framed as a way to deliver agency services securely. This would value information sharing goals based on how digital government can benefit citizens—rather than solely framed through a security lens that can drive a “need to protect” over a “need to share” approach.

In both the U.S. and EU, strong executive sponsorship for sharing has helped to translate data to action in a way that enables rapid response even when confronting bureaucratic challenges. Leaders can ensure that their teams have permission to collaborate quickly and effectively despite organizational hurdles, based on a set of agreed-upon guiding principles that help operators collaborate and move forward.

Upgrading Skills

Leaders need proper knowledge and skills to effectively champion change—this includes judges, policy makers, and procurement officials. With regard to judges, many decisions about the adequacy and propriety of information sharing are made in the courts, where choices rely on current knowledge and past case experience—which is inherently retrospective. Looking retrospectively when dealing with national and global security may limit information sharing instead of drawing on new innovations to enable decisions at speed. Expanding digital literacy among policy makers is critically needed to address this gap.

More broadly, education on modern technology needs to be spread through non-technical stakeholder organizations, specifically across legal, technology, and intelligence realms, to guard against what one EU stakeholder refers to as the “analog hangover effect.” Leaders need a broad, high-level understanding of how technology can help solve challenges, which would enable collaborative conversation, participation, and action across organizations. Consistent knowledge and skills within law, technology, and intelligence sectors will improve the transparency of communication and prepare leaders to come to the table in a way that points to a collective vision for change. Leaders from multiple stakeholder organizations must be informed on the challenges and possible solutions to make informed decisions.

In addition, the U.S. faces a specific challenge from the over-classification of threat information—a large bureaucratic process and resource investment drives the classification of information. Over-classification of threat information and intelligence constrains information access and sharing capabilities, and courts can also place constraints on information that inhibit efficient information sharing. At the same time, classified information can appear on open source or commercial threat feeds. Policies that promote security declassification based on minimal risk levels can help reduce bureaucratic steps and increase sharing at speed. For example, why classify an IP address absent a specific need? And where such need exists, standard operational procedures can be established to create a norm for the release of unclassified versions of data that can be shared. Through effective communication to stakeholders, leaders need to explain why information is classified—and what information should be shared under what processes. Adversaries move at full speed without these constraints. The U.S. and EU can protect information while also identifying approaches to move ahead in sharing information.

The Role of Private Sector Partners

Challenges within government create a need for external stimuli to promote a path toward improvement. Industry partners can demonstrate how private sector data integrity and sharing standards would facilitate much needed reforms. Public-private partnerships can drive new forms of digital data governance, and multinational corporations can help promote standards for transatlantic consistency for information sharing, security and privacy, and data integrity.

An overwhelming abundance of open-source data is generated and analyzed in private data networks. Specifically, in areas such as cybersecurity and critical infrastructure protection, the private sector often has more accurate and timely information and shares this more effectively than government. The increased importance of open-source data—especially social media-based data—relative to classified data can promote data sharing by avoiding the challenges of over-classification and the constraints limiting data to officials with security clearances. Sharing open-source data still has to address the other challenges of data security and data integrity, but it can avoid the challenges of classification.

For example, in addressing threats from potentially harmful air travelers, collaborating with the private sector proved to be more effective than if government had approached the situation on its own. A U.S. law passed after 9/11 requires airlines operating flights to, from, or through the United States to provide DHS' Customs and Border Protection (CBP) with certain passenger reservation data. This assists CBP in securing U.S. borders and facilitating safe and efficient international travel, made possible because private airlines collaborate with CBP. Government agencies in other programs could benefit from access to private sector data as they can gather threat data and develop rapid responses and long-term resiliency strategies.

EU collaboration and data sharing across sectors is not facilitated by legislation that drives collective action. In this context, the most effective solution involves governments working together with companies, rather than mandates that compel rigid structures. An effective model may exist in CBP's "Trade Days," in which the head of the agency collaborates with private sector partners to gain diverse perspectives on how to improve current processes. For this voluntary exchange to have mutual value, agencies must think about how collaboration can benefit companies as well, incentivizing their participation. There is strong evidence to support the value of public-private partnerships for sharing and securing data, but those partnerships are not guaranteed unless legislation or incentives actively facilitate relationships.

Finally, government must establish processes for efficient data sharing while respecting important civil rights, civil liberties, and privacy protections, in a manner consistent with GDPR and other privacy and data protection laws and policies. As technology enables the faster exchange of personal information by government and industry, all parties need to continue to develop proper protocols that promote public-private partnerships targeting bad actors while protecting individually identifiable data. Such partnerships are key for new forms of digital data governance. For example, the DHS Customs Trade Partnership Against Terrorism (CTPAT) is a voluntary public-private partnership program, which recognizes that government can provide the highest cargo security only through close cooperation with commercial stakeholders of the international supply chain. Participation in CTPAT helps the government and improves the bottom line, making it a win-win for both sides.

Governments can benefit extensively by learning from private sector best practices and policies to ensure data is shared securely, efficiently, and effectively.

CONCLUSION

Lessons to be Shared in Building Trust

The U.S. and EU can learn from each other's experiences to progress in secure information sharing, which reside on a foundation of mutual trust.

The EU faces a migration crisis and terrorist attacks cross Europe. These translate into top-down actions to progress in a faster way. Currently, the EU is working on creating a single European entry portal, implemented in May 2018 and available to all 28 member states and partners. Europol is also looking to set up a watch list. Integrating across these and similar initiatives will require expanded attention to the information sharing experience.

The U.S. and EU face similar challenges with interoperability and trust. DHS has been working with the EU on interoperability; the EU has taught DHS about the "once-only" policy, under which citizens must give information to government once, and then the government uses the information in a transparent manner. The EU has also made progress on information sharing between countries. Governments in this context must be specific about the content to be shared, its handling, and its acceptable use. Answering these basic questions can help resolve some challenges faced by the U.S., where agencies may try to solve the hardest problem in sharing and never develop a process that gets to basic "what, when, and who" details.

Ultimately, trust underpins any information sharing. Given the complex environment in which the U.S. and EU operate, building trust must be dynamically negotiated and not a "binary" condition. Trust is built by the successful exchange of information for a specific purpose, which requires specific content for an agreed upon time period. This concept has informed coalition warfighting, in which a joint command and control structure requires mutual trust in shared databases and control paths. Another model to learn from comes from successful supply chains, which require pre-negotiated sharing of control and data across enterprises. Thousands of partners share information, each for a specific purpose and time, and swap in and out frequently in a search for the best value and cheapest supplier. Finally, agency liaison officers can build trust through personal contact across data sharing boundaries.

The U.S. and EU can work together to combat these challenges in improving the information sharing enterprise across borders, making the world safer for all citizens.

ABOUT THE AUTHORS

DOUGLAS LUTE

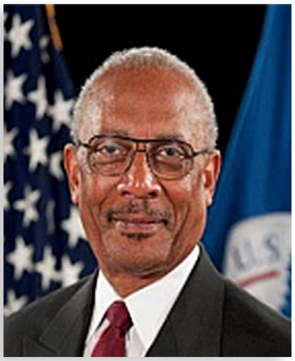
Ambassador Douglas Lute, Senior Fellow at the Belfer Center for Science and International Affairs at the Harvard Kennedy School of Government, is the former United States Permanent Representative to the North Atlantic Council, NATO's standing political body. Appointed by President Obama, he assumed the Brussels-based post in 2013 and served until 2017. During this period he was instrumental in designing and implementing the 28-nation Alliance's responses to the most severe security challenges in Europe since the end of the Cold War.

A career Army officer, in 2010, General Lute retired from active duty as a lieutenant general after 35 years of service. In 2007, President Bush named him as Assistant to the President and Deputy National Security Advisor to coordinate the wars in Iraq and Afghanistan. In 2009, he was the senior White House official retained by President Obama and his focus on the National Security Council staff shifted to South Asia. Across these two Administrations, he served a total of six years in the White House.

Before being assigned to the White House, General Lute served as Director of Operations (J3) on the Joint Staff, overseeing U.S. military operations worldwide. From 2004 to 2006, he was Director of Operations for the United States Central Command, with responsibility for U.S. military operations in 25 countries across the Middle East, eastern Africa and Central Asia, in which over 200,000 U.S. troops operated.

Through his military-diplomatic career he has received numerous honors and awards, including three awards of the Defense Distinguished Service Medal, the State Department's Distinguished Honor Award, the Grand Officer of the Order of Merit for the Italian Republic, and the Commander's Cross of the Order of Merit for the Federal Republic of Germany.

General Lute holds degrees from the United States Military Academy at West Point and from the Kennedy School of Government at Harvard University. He is also a member of the Council on Foreign Relations, a charter member of the Flag Officer Advisory Group of the United States Institute of Peace, and President of Cambridge Global Advisors.



FRANCIS TAYLOR

Francis X. Taylor, Executive Fellow of the Global Policy Initiative at the Keough School of Global Affairs at Notre Dame University, is the former Under Secretary for Intelligence and Analysis at the U.S. Department of Homeland Security. In that role, he provided the Secretary, DHS senior leadership, the DHS components, and state, local, tribal and private sector partners with the homeland security intelligence and information they needed to keep the country safe, secure, and resilient. I&A is a member of, and the Department's liaison to, the National Intelligence Community.

Prior to his assignment at DHS I&A, Mr. Taylor was Vice President and Chief Security Officer for the General Electric Company in Fairfield, Conn. At GE, he was responsible for managing the security operations and crisis management processes designed to ensure the security of GE employees and operations globally.

Before GE, Mr. Taylor had a distinguished 35-year career in government service, where he held several senior positions managing investigations, security, and counterterrorism issues.

Most recently, he served as the Assistant Secretary of State for Diplomatic Security and Director of the Office of Foreign Missions, with the rank of Ambassador. He was responsible for the global security of all U.S. diplomatic personnel and facilities. Mr. Taylor has served as the U.S. Ambassador at Large and Coordinator for Counterterrorism for the Department of State from July 2001 to November 2002. In this role, he was responsible for implementing U.S. counterterrorism policy overseas and coordinating the U.S. government response to international terrorist activities.

During his 31 years of military service, Ambassador Taylor served with distinction in numerous command and staff positions, rising to the rank of Brigadier General in September 1996. In his final active duty assignment, Brigadier General Taylor was the Commander, Air Force Office of Special Investigations, responsible for providing Air Force leaders with comprehensive criminal, fraud, counterintelligence and security investigation and operations to protect global Air Force operations.

Mr. Taylor has received numerous awards and decorations, including the U.S. Distinguished Service Medal, the National Intelligence Distinguished Service Medal, the Legion of Merit, the Defense Superior Service Medal, and the U.S. Department of State Honor Award.

Mr. Taylor holds a Bachelor's and Master's Degree in Government and International Studies from the University of Notre Dame. He is a Distinguished Graduate of the Notre Dame Air Force ROTC program. He is also a Principal with Cambridge Global Advisors.

ACKNOWLEDGEMENTS

This report results from great insights shared by global leaders who attended the two roundtables that provided a rich content base for the authors to draw on, and we thank each attendee listed in the Appendix for their contribution. In addition, the report authors and the IBM Center would like to especially thank several individuals who helped shape the content and preparation for these roundtables and this report:

- Nate Snyder, Jacob Braun, Morgan Ryan, and Chris Cummiskey, former DHS officials now with Cambridge Global Advisors
- John Zangardi, Donna Roy, and Michael Scardaville with the U.S. Department of Homeland Security
- Robert Paschall and Kamila Slanska with the U.S. Mission to the European Union
- Nicole Johnson and Sydney Mann with IBM Global Business Services
- Ruth Gordon with the IBM Center for The Business of Government

APPENDIX: ROUNDTABLE PARTICIPANTS

Washington, D.C. October 27, 2017

David Ashley
Chief Data Officer for Human Capital
Department of Homeland Security

Jake Braun
CEO, Cambridge Global Advisors
(Former Director of White House and Public
Liaison Department of Homeland Security)

Chris Calabrese
Vice President for Policy
Center for Democracy & Technology

Dan Chenok
Executive Director
IBM Center for The Business of Government

Chris Cummiskey
Senior Advisor, Cambridge Global Advisors
(Former Acting Under Secretary for
Management Department of Homeland
Security)

Curtis Dukes
Executive Vice President and General Manager,
Security Best Practices & Automation Group,
Center for Internet Security
(Former Director of Information Assurance
Directorate, National Security Agency)

Don Fenhagen
Partner, IBM

John Gilligan
Chairman
Center for Internet Security

Nicole Johnson
Consultant, IBM

Andrew Kuepper
Deputy Assistant Secretary
Unity of Effort Integration
Department of Homeland Security

Connie LaRossa
National Security Consultant, Deloitte
(Former Deputy Assistant Secretary of
Legislative Affairs, Department of
Homeland Security)

Douglas Lute
Lieutenant General US Army (Retired)
Former U.S. Ambassador to NATO

Sydney Mann
Consultant, IBM

Phil McNamara
Consultant
(Former Assistant Secretary for
Intergovernmental Affairs, Department of
Homeland Security)

Brad Nix
Acting Director of US-CERT
Department of Homeland Security

Pablo Pelaez
Europol Representative to the U.S.

Todd Rosenblum
Former Principal Deputy/Acting Assistant
Secretary for Homeland Defense,
Department of Defense; and
Former Deputy Undersecretary
of Intelligence, Department of Homeland
Security

Donna Roy
Executive Director, Information Sharing
and Services Office
Department of Homeland Security

Morgan Ryan
Vice President for Client Services
Cambridge Global Advisors

Tony Sager
Senior Vice President, Center for Internet
Security (Former Chief Operating Officer for the
Information Assurance Directorate
National Security Agency)

Mike Scardaville
Principal Director, Information Sharing Policy
Department of Homeland Security

Sonny Sinha
Principal, Sinha Associates LLC
(Former Special Assistant and Senior
Congressional Adviser for Cybersecurity National
Protection and Programs Directorate's
Cybersecurity and Communications Office
Department of Homeland Security)

Brenda Smith
Executive Assistant Commissioner
Office of Trade
Customs and Border Protection

Nate Snyder
Senior Advisor
Cambridge Global Advisors
(Former Principal Senior Advisor & Chief of Staff
for Policy, Office for Community Partnerships,
Department of Homeland Security)

Frank Taylor
Brigadier General US Air Force (Retired)
Former Under Secretary for I&A
U.S. Department of Homeland Security

Leendert Van Bochoven
Global Lead for Defense and Intelligence, IBM

Bryan Whitaker
Chief Innovation Officer
TargetSmart

Brussels, Belgium. February 22, 2018

Christina Bell
International Advisor
U.S. Customs and Border Protection

Jason A. Biros
Legal Adviser
U.S. Mission to the European Union

Daniel Chenok
Executive Director
The IBM Center for The Business of
Government

Jeffrey DaRin
Attache
Homeland Security Investigations

Cindy Degreef
Liaison Officer
eu-Lisa

Brian Donald
Chief of Staff
Europol

Sorin Ducaru
Ambassador
Senior Fellow, Hudson Institute
Former NATO Assistant Secretary General
for Emerging Security Challenges

Don Fenhagen
Partner
IBM

Florent Frederix
Principal Administrator
Trust and Security Unit
European Commission (DG Connect)

Luukas Ilves
Deputy Director and Senior Fellow
The Lisbon Council

Jean-François Junger
Deputy Head of Unit
DG Connect

Robert Keil
Branch Head/Software Development
Federal Office of Migration and Refugees

Christian Lifländer
Head, Cyber Defence Section
Emerging Security Challenges Division
NATO

Douglas Lute
Lieutenant General US Army (Retired)
Former U.S. Ambassador to NATO

Paul McKeown
Government Solutions Centre of
Competence, Borders and Immigration
Management Segment Leader
IBM

Sandra Nunes
Head of Sector, Liaison Office Brussels
eu-LISA

Bob Paschall
Regional Attaché for Europe and The U.S.
Mission to the EU
Department of Homeland Security
U.S. Embassy Brussels

Ben Pugsley
Advisor
Council of the European Union

James Reynolds-Brown
Cyber Defense Policy Officer
NATO

Donna Roy
Executive Director, IS2O
U.S. Department of Homeland Security

Emmanuel Saliot
Advisor
Council of the European Union

Darek Saunders
Head of Analytics Sector
Analytics in Risk Analysis Unit
European Border and Coast Guard Agency
Frontex

Pedro Serrano
Deputy Secretary General
European External Action Service

Adam Shub
Chargé d'Affaires
U.S. Mission to the European Union

Kamila Slanska
Program Manager
Homeland Security Investigations

Nate Snyder
Senior Advisor
Cambridge Global Advisors

Erich Staudacher
General Manager
AFCEA Europe

Francis X. Taylor
Brigadier General US Air Force (Retired)
Former Under Secretary for I&A
U.S. Department of Homeland Security

Paul Timmers
Visiting Research Fellow of Cybersecurity
Oxford University

Chris Treib
Special Advisor to the DHS CIO
Office of the Chief Information Officer
U.S. Department of Homeland Security
Commander, U.S. Coast Guard

Leendert Van Bochoven
Global Lead for Defense and Intelligence,
IBM

John Zangardi
CIO
U.S. Department of Homeland Security

KEY CONTACT INFORMATION

To contact the authors:

Douglas Lute

Senior Fellow, Harvard Belfer Center for Science and International Affairs

Cambridge Global Advisors

1700 N. Moore St #2100

Arlington, VA 22209

Francis Taylor

Executive Fellow, Keough School of Global Affairs
University of Notre Dame

Cambridge Global Advisors

1700 N. Moore St #2100

Arlington, VA 22209?

REPORTS FROM THE IBM CENTER FOR THE BUSINESS OF GOVERNMENT

For a full listing of our publications, visit www.businessofgovernment.org

Recent reports available on the website include:

Acquisition

Ten Actions to Improve Inventory Management in Government: Lessons From VA Hospitals by Gilbert N. Nyaga, Gary J. Young, and George (Russ) Moran

Beyond Business as Usual: Improving Defense Acquisition through Better Buying Power by Zachary S. Huitink and David M. Van Slyke

Collaborating Across Boundaries

Cross-Agency Collaboration: A Case Study of Cross-Agency Priority Goals by John M. Kamensky

Interagency Performance Targets: A Case Study of New Zealand's Results Programme by Dr. Rodney Scott and Ross Boyd

Improving Performance

Seven Drivers Transforming Government by Dan Chenok, Haynes A. Cooney, John M. Kamensky, Michael J. Keegan, and Darcie Piechowski

Five Actions to Improve Military Hospital Performance by John Whitley

A Framework for Improving Federal Program Managementby by Janet Weiss

Innovation

Tiered Evidence Grants - An Assessment of the Education Innovation and Research Program by Patrick Lester

A Playbook for CIO-Enabled Innovation in the Federal Government by Gregory S. Dawson and James S. Denford

Making Open Innovation Ecosystems Work: Case Studies in Healthcare by Donald E. Wynn, Jr., Renée M. E. Pratt, and Randy V. Bradley

Leadership

Best Practices for Succession Planning in Federal Government STEMM Positions by Gina Scott Ligon, JoDee Friedly, and Victoria Kennel

Risk

Risk Management and Reducing Improper Payments: A Case Study of the U.S. Department of Labor by Dr. Robert Greer and Justin B. Bullock

Ten Recommendations for Managing Organizational Integrity Risks by Anthony D. Molina

Managing Cybersecurity Risk in Government by Rajni Goel, James Haddow and Anupam Kumar

Using Technology

Delivering Artificial Intelligence in Government: Challenges and Opportunities by Kevin C. Desouza

Using Artificial Intelligence to Transform Government by The IBM Center for The Business of Government and the Partnership for Public Service

Digital Service Teams: Challenges and Recommendations for Government by Professor Dr. Ines Mergel

Ten Actions to Implement Big Data Initiatives: A Study of 65 Cities by Alfred T. Ho and Bo McCall

The Social Intranet: Insights on Managing and Sharing Knowledge Internally by Dr. Ines Mergel

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

About IBM Global Business Services

With consultants and professional staff in more than 160 countries globally, IBM Global Business Services is the world's largest consulting services organization. IBM Global Business Services provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value. To learn more visit ibm.com.

For more information:
Daniel J. Chenok
Executive Director
IBM Center for The Business of Government

600 14th Street NW
Second Floor
Washington, DC 20005
202-551-9342

website: www.businessofgovernment.org
e-mail: businessofgovernment@us.ibm.com

Stay connected with the IBM Center on:

govloop YouTube

or, send us your name and e-mail to receive our newsletters.

IBM Center for
The Business of Government

20 years of research for government:
informing today, envisioning tomorrow

1998-2018