NATIONAL ACADEMY OF PUBLIC ADMINISTRATION®

Managing Technological Changes:

A Spotlight Report

Academy Staff 2021
Working Paper:
Ensure Data Security and Privacy
Make Government AI-Ready

Spotlight Report on Managing Technological Changes

Introduction

In November 2019, the National Academy of Public Administration (the Academy) announced 12 Grand Challenges in Public Administration after a year of intense research under the guidance of a Steering Committee from across the field.

Focus Area	**Grand Challenge**
Managing Technological Changes	1. Ensure Data Security and Privacy Rights of Individuals 2. Make Government AI Ready
Protecting & Advancing Democracy	3. Protect Electoral Integrity and Enhance Voter Participation 4. Modernize and Reinvigorate the Public Service 5. Develop New Approaches to Public Governance and Engagement 6. Advance National Interests in a Changing Global Context
Strengthening Social & Economic Development	7. Foster Social Equity 8. Connect Individuals to Meaningful Work 9. Build Resilient Communities 10. Advance the Nation's Long-Term Fiscal Health
Ensuring Environmental Sustainability	11. Steward Natural Resources and Address Climate Change 12. Create Modern Water Systems for Safe and Sustainable Use

This spotlight report focuses on the Grand Challenges, Ensure Data Security and Make Government AI Ready.   This working paper is a follow-up to the Election 2020 reports produced by Academy Fellows and also documents some illustrative actions underway at the state and local levels. This paper is a work-in-progress that will be expanded upon in 2022, especially through a greater focus on non-federal actions.

The Current State

Technology in the Digital Age offers a great opportunity for the government to better serve its citizens and solve some of the government's "wicked problems" more quickly and effectively, but first, public administrators must ensure that they address the multitude of risks to citizens' economic, security, and privacy interests. Throughout the twenty-first century and especially in the past few years, the threats to the data security of American public and private firms have increased. State and non-state actors have targeted oil pipelines, water treatment plants, and even data platforms of federal agencies in attempts to gain material resources and information.

At the same time, these competitors, which include China and Russia, are developing Artificial Intelligence (AI) tools to facilitate both these cyberattacks and a larger technology agenda. While authoritarian regimes can research and wield these AI tools without regard for their citizens' privacy, the U.S. must simultaneously produce equal or better technology while ensuring the safety, trustworthiness, and transparency of this technology are within the boundaries of the constitution and legislation. These technology Grand Challenges are intertwined, and the U.S. must solve them in order to produce a strong, safe, and reliable foundation for its citizens in this new era.

ENSURING DATA SECURITY AND PRIVACY

Modernizing data security systems and protecting classified information from foreign actors and adversaries have become huge problems for the United States in recent years. The need for modernization has never been greater, as there has been a marked increase in cyber-attacks from international adversaries, notably Russia, China, and North Korea, against various company and government data operations in recent years. In the past year alone, cyber-attacks against companies and governments increased ten-fold.[1] Over the past couple of years, the North American countries have had a 158 percent rise in ransomware.[2] Attacks on operational technology also increased significantly, with incidents disrupting supply chains, critical infrastructure functionality, and services the American public relies on for day-to-day activities.[3]

Such hacks harm our economy and pose a national security threat. Recent attacks on American corporations include those on the Colonial Pipeline and JBS. The attack on the pipeline shuttered gas stations and increased prices up and down the East Coast,[4] while the hack on JBS shut down operations at the world's largest meat processor, disrupting the global supply chain.[5] These attacks demonstrate that blackmail operations have become an increasingly common form of hacking with impacts directly felt by the American public.

Over the last few years, hackers have also targeted government agencies, schools, and hospitals in their cyberattacks.[6] In May, Nobelium, the Russian firm behind the Solar Winds breach, conducted a cyberattack against the U.S. Agency for International Development (USAID).[7] Nobelium targeted USAID's Constant Contact account and sent out an "intelligence-gathering phishing campaign targeting 3,000 email accounts at more than 150 organizations, including other agencies, think tanks, contractors, and non-governmental organizations."[8]

Cyberattacks are difficult to deter. U.S. agencies have difficulty tracking the crime itself as well as the payments made from the targeted companies to the hackers.[9] The usage of cryptocurrencies as the preferred payment for hackers hinders authorities tracking abilities.[10] In the face of these obstacles, many targets feel forced to pay the hackers.[11]

- JBS paid $11 million in bitcoin.[12]
- Colonial paid $4.4 million in bitcoin.[13]

- The FBI was able to recover $2.3 million of the bitcoin paid by Colonial Pipeline, but it is not publicly available how consistent U.S. agencies can recover these ransoms.[14]

Both organizations paid the hackers initially because it often costs more money to rebuild than to pay the ransom. The city of Baltimore is another example:

- The computer systems for the city of Baltimore were hacked with a ransom of $760 thousand in bitcoin.
- The mayor refused to pay, but the cost of rebuilding computer systems for the city government has so far reached $18.2 million.[15]

Publicly, the FBI advises victims not to pay a ransom to discourage perpetrators from targeting more victims, but privately they will tell targets that they understand if they feel the need to pay.[16]

Local governments are not immune to these attacks either. In February, a person hacked into the water system of Oldsmar, Florida and tried to increase the levels of sodium hydroxide in the city's water, putting thousands at risk of being poisoned.[17] The Pinellas County Sheriff's Office, the FBI, and the Secret Service are still in the process of jointly investigating the breach.

ARTIFICIAL INTELLIGENCE

Artificial Intelligence (AI) allows computerized systems to perform tasks traditionally requiring human intelligence: analytics, decision support, visual perception, and foreign language translation. AI and Robotics Process Automation (RPA) have the potential to spur economic growth, enhance national security, and improve the quality of life. In a world of “Big Data” and “Thick Data,” AI tools can process huge amounts of data in seconds, automating tasks that would take days or longer for human beings to perform.

The public sector in the United States is at the very beginning of a long-term journey to develop and harness these tools. Chatbots are being used in citizen engagement systems; AI technology is augmenting decision-making in the areas of cyber security monitoring, public policy modeling, database anomalies, and waste and abuse identification. It will affect the workdays of employees at all levels of government as AI can accomplish routine, repetitive tasks and allow employees to more closely focus on the agency’s core mission. Harnessing AI will deliver more personalized services to citizens, and it will deliver those services more quickly. More effective administration of government through AI may even lead to other benefits such as more public trust in government to do its job.

AI in the public sector can yield numerous benefits, but its advancement must come from a solid foundation of management. AI raises the following concerns about trustworthiness, security, and transparency:

- With biased or inaccurate data, AI systems will produce unequitable results.
- Cybersecurity will be more important than ever to protect against malicious actors that, by taking over AI systems, could do significant damage very quickly.

- Without transparency, the public may be confused about how key decisions were made, which could further the public's distrust in public agencies as well as the technology itself.
- Governments may need to revamp their budgeting and procurement processes to be able to quickly acquire and deploy advanced technologies that can iterate much faster than the current budget cycle.

As we learn more about AI, more concerns arise over its trustworthiness including the accuracy of the AI's data and the bias of its data. Accuracy of data input into AI will be crucial to the safe and successful use of this technology in functions like autonomous vehicles and AI-enhanced medical devices. AI using biased data can produce discriminatory results in functions such as hiring, or mortgage or rental loans. AI tools and AI-enhanced tools can indeed be a powerful facilitator for many tasks. The U.S. must ensure, however, that these tools have sufficient accuracy and have minimization of bias to use them.

As with many technological innovations used by the government, transparency in the use of AI is paramount to achieving public trust in its functions. Citizens cannot trust AI produced results without first trusting the tool itself. Since AI is a progress compounding technology, the U.S. must include transparency measures at the start of AI's usage and throughout each iteration of its evolution.

AI will be a major contributor to the security of the U.S., but it will also be wielded by malevolent actors against U.S. interests. The National Security Commission on Artificial Intelligence (NSCAI) stated that, "AI systems will also be used in the pursuit of power" by both state and non-state actors and through different functions including dis- and misinformation campaigns and AI enabled "smart weapons."[18] Not only must the U.S. establish practices that consistently produce trustworthy and transparent AI, but it must also do so quickly. China, Russia, and other state and non-state competitors, who many times do not need to consider similar privacy measures as the U.S., are also heavily focused in this area. The need for the U.S. to have at least equal capabilities is critical to securing America and its interests in the 21st century. Yet, the NSCAI reported that the U.S. is lacking in developing its technical infrastructure, human talent, and innovation investment toward making government AI-ready.[19] The timetable for the U.S. to confirm its competitiveness and possibly superiority in technology is shrinking. Since these AI tools are so powerful and their progress compounding, a proper foundation now is critical to successful protection of American citizens and interests in the future. "Catching-up" to global competitors at a later date will be extremely difficult.

Actions Underway

Governments at all levels in the U.S. have taken measures to align new technology with their functions. Even the more basic AI can now be found in government services such as the filing of forms, while governments are recognizing the major threats to their systems through cybersecurity. Resources and legislation have focused on security, the technology workforce, investments in research and development, and technical infrastructure.

FEDERAL GOVERNMENT

The federal government has responded to the challenges in the Digital age through several actions including instituting security standards and frameworks, investments in the workforce and human talent, standards for technology:

Security

- **E.O. 14028: Improving the Nation's Cybersecurity**[20] seeks to
    - Coordinate government, especially executive agencies, efforts and reduce compartmentalization of cyber risk and attack response within the federal government through the usage of the NIST security framework.
    - Instruct agencies to adopt multi-factor authentication and encryption of data and direct the heads of Federal Civilian Executive Branch Agencies to provide reports to the Secretary of Homeland Security through the Director of Cybersecurity and Infrastructure Security Agency (CISA), the Director of the Office of Management and Budget (OMB), and the Assistant to the President for National Security Affairs (APNSA) on their respective agencies' progress in adopting multi-factor authentication and encryption of data that is at rest.
    - Instruct the Federal government to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software
    - Require the Secretary of DHS to work with the Attorney General to establish the Cyber Safety Review Board.

  Parts of this E.O. are in alignment with the recommendation of the Academy's Working Group on Ensuring Data Security which stressed the importance of the implementation of government data privacy policies' including the exploration of trade-offs of cross-agency data sharing and authentication.

- **E.O. 14034: Protecting Americans Sensitive Data from Foreign Adversaries**[21] focused on protecting consumers' data from outside sources. It included the following actions:
    - Rescinded former President Trump's executive order that banned TikTok and WeChat
    - Initiated a review of national security risks associated with software application with ties to China
    - Directed the Department of Commerce to undertake an evidence-based analysis of transactions involving apps that are manufactured, supplied or controlled by China.
    - Required that the Secretary of Commerce in consultation with the heads of State, Defense, Justice, DHS, HHS, and ODNI provide a report to the National Security Advisory with recommendation to "protect against harm from the unrestricted sale of, transfer of, or access to United States persons' sensitive data."

    - Directed the DNI to provided threat assessments and the Secretary of DHS to provide a vulnerability assessment, using information they glean from the recommendations.
- **The Biden Administration is working with the National Institute of Standards and Technology (NIST) and industry partners to develop a new framework** to improve the security of the technology supply chain.[22] The framework will serve as a "guideline to public and private entities on how to build secure technology and assess the security of technology, including open-source software."

  This initiative touches on the recommendation by the Academy Working Group in their report, Ensure Data Privacy and Security, to establish a cybersecurity workforce advisory commission that would serve to review existing frameworks and recommendations in addition to developing new frameworks and career paths for federal cybersecurity.

- **The National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems** directs CISA and NIST to develop cybersecurity performance goals for critical infrastructure that would be used as guidance for essential service companies.[23]

- **Other Federal cybersecurity actions include**:
    - The Transportation Security Administration (TSA) issued a security directive that addresses issues raised by the Colonial Pipeline hack by requiring that pipeline companies report cyber incidents to the Federal government.[24] This directive also requires owners and operators of TSA-designated critical pipelines that transport hazardous liquid and natural gas to implement a number of protections against cyber intrusions.
    - The Technology Modernization Fund received $1 billion in the American Rescue Plan to address pressing modernization and cybersecurity needs in government agencies.[25]

Innovation

- **E.O. 13960: Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government[26],** ordered in December of 2020, encourages alignment of Federal agencies with AI technology within the ethical boundaries and legal framework of E.O. 13859[27], ordered in February of 2019. The Biden Administration in September of 2021 also established a **National Artificial Intelligence Advisory Committee (NAIAC)** under the Department of Commerce.[28] The NAIAC, which was created under the guidance of the National AI Initiative Act of 2020, will advise the White House on a number of AI-related issues including:[29]
    - Establishing standards that require equitable treatment and racial justice in the development of AI
    - Ensuring that advances in AI are matched with advances in trustworthiness, fairness, and protection of civil rights

- Assessing the current competitiveness of U.S. AI

These initiatives follow the recommendations of the Academy Working Group on Making Government AI Ready to:

- build trustworthy AI by establishing a federal entity focused on the effects of AI;
- use ethical frameworks to identify and reduce bias in AI by demonstrating a federal government commitment to ethical principles and standards in AI development and use, and;
- build intergovernmental partnerships and knowledge sharing around public sector uses of AI.

These initiatives, while just in the beginning stages, have the potential to achieve the Working Group's standards and provide a management foundation for future AI technologies.

Workforce and Human Talent

- **The FY 2021 National Defense Authorization Act (NDAA)** included twenty-five of the Cyberspace Solarium Commission's recommendations.[30] These recommendations include establishing a Cyber Security Director, strengthening CISA, identifying certain sector specific agencies as risk management agencies for their respective sectors, and creating a Joint Cyber Planning Office.

  The inclusion of the Commission's recommendations in the NDAA aligns with the recommendation of the NAPA Working Group's report, Ensure Data Privacy and Security, to build upon the Cyberspace Solarium Commission and begin acting on its recommendations.

- **OMB has launched a data reskilling program**, which seeks to train current government employees on in-demand technology techniques.[31] The goal is to increase the skill base of these employees, while conserving resources on the recruitment and training of new talent. In a similar action, the Chief Information Officer of OPM has brokered a deal with Microsoft to provide free, high-quality IT training for all OCIO employees.[32] He also gave a directive to OCIO employees to take an introduction to the cloud class, even if they are not tech employees.

  These programs align with the recommendation of the Working Group's report, Ensure Data Privacy and Security to develop a hands-on cybersecurity training and reskilling program for federal employees who do not work in IT.

- **E.O. 13960: Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government** briefly mentions the development of AI-ready workforce, but it does not order specific action.[33]

This E.O. may spark further discussion on the AI workforce. The Academy's Working Group on Make Government AI-Ready recommended that the Federal Government "build an AI-ready workforce by providing funding to support the growth of an AI competent federal workforce, develop policies and fund incentives that encourage the AI R&D to use multidisciplinary teams, and support studies to increase understanding of current and future national workforce needs for AI R&D."

STATE AND LOCAL GOVERNMENTS

Security

Some states have enacted laws to protect consumer's data in the absence of comprehensive federal legislation:

- California, through the California Consumer Privacy Act (CCPA), most recently amended in 2020, enables users to opt out of personal data tracking, to command companies to delete all collected information, and to sue technology firms for misuse.[34]
- Virginia's privacy law creates protections for consumers to better control their data and establishes that companies must disclose their collection of data and to delete data if instructed by the consumer.[35]
- The Colorado State Legislature recently passed the "Colorado Privacy Act,", which gives residents the right to tell companies to stop collecting their data and delete personal data.[36]

There have been multiple state initiatives with the intent to strengthen the trustworthiness of AI.

- The city of Baltimore passed an ordinance in January of 2021 banning facial recognition technology in both the private and public sectors.[37]
- Several cities including San Francisco, CA; Boston, MA; Portland, ME; Portland, OR; Springfield, MA; Alameda, CA; Berkeley, CA; Brookline, MA; Cambridge, MA; Northampton, MA; Somerville, MA; and Jackson, MI have banned police from using facial recognition.[38]
- In July of 2021, Illinois mandated that their Artificial Intelligence Video Interview Act must require the Department of Commerce and Economic Opportunity to analyze data to ensure that employers depending on AI to ward interviews are not racially biased[39]
- Colorado banned insurers from using any algorithms or external consumer data sources that unfairly discriminate based on many factors.[40]
- Washington has enacted a law governing the use of facial recognition AI measured by public entities. Any state agencies that use these technological measures must test the programs for accuracy.[41]

Workforce

Some state governments are revamping their IT and AI workforce through retraining and education programs.

- Virginia is sponsoring a VA Cyber Skills Academy, which was created to help residents learn new technical skills and meet the high demand for cybersecurity professionals.[42]
- Maryland has given more funding to the SANS Cyber Workforce Academy in order to reskill and upskill the academy, which is focused on Maryland residents and veterans.[43]
- Mississippi has manded K-12 computer science curriculum that includes AI learning.[44]

INTERNATIONAL

Issues in technology are globally interconnected. Cyber-attackers can now strike from anywhere in the world, and technology produced in the U.S. is now traded overseas. To more efficiently and safely defend against cyberattacks and to facilitate the trade of AI and other technologies with our international partners, the U.S. must engage countries on bilateral and multilateral levels.

In the cybersecurity realm, CISA plays a large role in forming a global security cooperation among the U.S. and its allies. CISA's "CISA Global" strategy seeks to protect U.S. critical infrastructure and identify emerging threats through the following objectives with its partners:[45]

- **Operational Cooperation:** 1) Assess and counter evolving risks, and 2) strengthen the security and resilience of U.S. critical infrastructure
- **Capacity Building:** 1) Increase partner capacity and awareness
- **Stakeholder Engagement and Outreach**: 1) Enhance shared understanding of threats and preparedness for response, and 2) Advance global operational public-private coordination
- **Shaping the Policy Ecosystem:** 1) Advance U.S. Interest in International Fora, and 2) Develop capabilities and standards that support U.S. interests

It is also important for the U.S. to engage with its international partners on issues surrounding AI development. Although the U.S. has bilateral cooperation agreements with countries like the U.K., much of the international cooperation between U.S. and other countries and the U.S. and international institutions is less direct. The U.S. engages other countries through forums revolving around shared values like the G-7 Science and Technology Ministerial Meeting that launched the Global Partnership on AI.[46] The U.S. also adopts measures regarding trustworthiness and privacy that are agreed upon by international organizations like the Organization for Economic Cooperation and Development (OECD).

The U.S. must also engage with its partners in the European Union (E.U.) to ensure that any differences in standards in AI between the two entities do not severely disrupt the trading of AI-enhanced technologies. The E.U. recognized the importance of this relationship as well in a white paper by the European Commission entitled, "New EU-US Agenda for Global Change."[47] The paper called on more collaboration between the U.S. and E.U. to establish bilateral and multilateral levels of cooperation based on trust, the free flow of data, and "the basis of high standards and safeguards."

Conclusion

The purpose of this staff working paper was to follow-up on the Election 2020 Working Group reports for the federal Administration by highlighting key actions intended to address these Grand Challenges. The Academy staff welcomes Fellow input and advice, especially on steps being undertaken by especially states, localities, and Tribes. Over the next year, this paper will update information on federal actions based on the latest information and place a greater emphasis on non-federal actions.

ACADEMY STAFF AUTHORS

Joe Mitchell, *Director of Strategic Initiatives and International Programs*. Dr. Mitchell has worked with a wide range of federal cabinet departments and agencies to develop higher-performing organizations, implement organizational change, and strengthen human capital and teams. He currently leads the Academy's thought leadership activities, including its Grand Challenges in Public Administration, and co-leads its Agile Government Center. Most recently, he served at the General Services Administration to stand up the Office of Shared Solutions and Performance Improvement within the Office of Government-wide Policy, where he led a team that performed multi-functional, cross-agency projects and initiatives in support of the President's Management Agenda. Previously, he led and managed the Academy's organizational studies program, providing strategic direction and project oversight to all of its congressionally-directed and agency-requested reviews and consulting engagements. He holds a Ph.D. from the Virginia Polytechnic Institute and State University, a Master of International Public Policy from the Johns Hopkins University School of Advanced International Studies, a Master of Public Administration from the University of North Carolina at Charlotte, and a B.A. in History from the University of North Carolina at Wilmington.

James Higgins, *Senior Research Associate*. Mr. Higgins joined the Academy in March 2020. He currently supports the Academy's strategic initiatives, including the Grand Challenges in Public Administration, Agile Management projects, and the Management Matters: Where Policy Meets Practice podcast. He supported the Academy Fellow Election 2020 Working Groups and has been a key staff member of the Agile Government Center. He holds a Master's in Global Policy from the University of Maine's School of Policy and International Affairs and a B.A. in International Studies from Dickinson College.

Jillian McGuffey, *Research Associate*. Ms. McGuffey joined the Academy's Strategic Initiatives Team in December 2020. She manages the Academy's federalism website, conducted a wide range of research for the Grand Challenges in Public Administration, and helped produce the Management Matters podcast. During her undergraduate career, Jillian was selected as a fellow of the Global Fellows Program, which gave her various opportunities to learn from experts specializing in international relations and conflict resolution. She also worked with the United States Census Bureau, where she recorded and analyzed data from the 2017 Criminal Juvenile Resident Placement Survey, and the USCIS supporting efforts to formulate DHS emergency preparedness plans. Ms. McGuffey graduated from the University of Maryland with a Master of Public Policy after earning a Bachelor of Arts in Government and Politics and a Minor in Creative Writing.

Additional Assistance Provided by Academy Interns:

Dywanique Ford: Junior at Virginia Polytechnic Institute and State University, pursuing dual degrees in National Security & Foreign Affairs and Criminology.

Madison Garofalo: Junior at Illinois Wesleyan University getting her B.A. in Political Science with a minor in Psychology.

Noah Jaffe: Senior at Denison University, receiving his Bachelor of Arts in History and Political Science.

Elizabeth LoBello: Senior at the University of Maryland, College Park, studying Public Policy.

Simon Sandt: Senior at the University of Bonn in Germany pursuing a major in Political Science and minor in Economics.

References

[1] Richberg, Jim. “If Government Leaders Aren’t Worried About Ransomware, They Should Be.” GovExec. October 12, 2021. https://www.govexec.com/technology/2021/10/if-government-leaders-arent-worried-about-ransomware-they-should-be/186036/.

[2] “Ransomware Soars with 62% Increase since 2019.” Security Magazine RSS. Security Magazine, March 16, 2021. https://www.securitymagazine.com/articles/94831-ransomware-soars-with-62-increase-since-2019.

[3] Richberg, Jim. “If Government Leaders Aren’t Worried About Ransomware, They Should Be.” GovExec. October 12, 2021. https://www.govexec.com/technology/2021/10/if-government-leaders-arent-worried-about-ransomware-they-should-be/186036/.

[4] “Age of the Cyber-Attack: US Struggles to Curb Rise of Digital Destabilization.” The Guardian. Guardian News and Media, June 14, 2021. https://www.theguardian.com/technology/2021/jun/14/age-of-the-cyber-attack-us-digital-destabilization.

[5] Ibid.

[6] Lonas, Lexi. “Iowa College Closed for Fourth Day after Cyberattack.” TheHill. June 8, 2021. https://thehill.com/blogs/blog-briefing-room/news/557310-iowa-college-closed-for-fourth-day-after-cyberattack?rl=1.

[7] Mitchell, Billy. “USAID Hit with Cyberattack by Russian-Backed Group Nobelium: Microsoft.” FedScoop, July 29, 2021. https://www.fedscoop.com/usaid-breached-in-new-russian-cyberattack/.

[8] Ibid.

[9] “Age of the Cyber-Attack: US Struggles to Curb Rise of Digital Destabilization.” The Guardian. Guardian News and Media, June 14, 2021. https://www.theguardian.com/technology/2021/jun/14/age-of-the-cyber-attack-us-digital-destabilization.

[10] Ibid.

[11] Ibid.

[12] Bunge, Jacob. “JBS Paid $11 Million to Resolve Ransomware Attack.” The Wall Street Journal. Dow Jones & Company, June 10, 2021. https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781.

[13] Ibid.

[14] Christopher Bing, Joseph Menn, Sarah N. Lynch. "U.S. seizes $2.3 mln in bitcoin paid to Colonial Pipeline hackers." Reuters. June 7, 2021. https://www.reuters.com/business/energy/us-announce-recovery-millions-colonial-pipeline-ransomware-attack-2021-06-07/.

[15] Duncan, Ian. "Baltimore Estimates Cost of Ransomware Attack at $18.2 Million as Government Begins to Restore Email Accounts." baltimoresun.com. Baltimore Sun, June 30, 2019. https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html.

[16] "Age of the Cyber-Attack: US Struggles to Curb Rise of Digital Destabilization." The Guardian. Guardian News and Media, June 14, 2021. https://www.theguardian.com/technology/2021/jun/14/age-of-the-cyber-attack-us-digital-destabilization.

[17] Cisco. "Oldsmar's Cyber Attack Raises the Alarm for the Water Industry." GovTech. April 23, 2021. https://www.govtech.com/sponsored/oldsmars-cyber-attack-raises-the-alarm-for-the-water-industry.html.

[18] "Final Report," National Security Commission on Artificial Intelligence. 2021. https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

[19] Ibid.

[20] "Executive Order on Improving the Nation's Cybersecurity." The White House. The United States Government, May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[21] "Protecting Americans' Sensitive Data from Foreign Adversaries." Federal Register. June 9, 2021. https://www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries

[22] "Fact Sheet: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity." The White House. The United States Government, August 25, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/.

[23] "National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems." The White House. The United States Government, July 28, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/.

[24] "DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators." DHS announces new cybersecurity requirements for critical pipeline owners and operators | Transportation Security Administration, July 20, 2021. https://www.tsa.gov/news/press/releases/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline.

[25] Mitchell, Billy. "White House Allocates $9.8B to Cybersecurity in 2022 Budget Request." FedScoop, September 1, 2021. https://www.fedscoop.com/white-house-allocates-9-8b-to-cybersecurity-in-2022-budget-request/.

[26] “Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government,” National Archives: Federal Register, December 8, 2020, https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government.

[27] ”Maintaining American Leadership in Artificial Intelligence,” National Archives: Federal Register, February 14, 2019, https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence.

[28] ”Department of Commerce Establishes National Artificial Intelligence Advisory Committee”, United States Department of Commerce, September 8, 2021, https://www.commerce.gov/news/press-releases/2021/09/department-commerce-establishes-national-artificial-intelligence.

[29] Ibid.

[30] “H.R.6395 - 116th Congress (2019-2020): William M...” January 01, 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395.

[31] “OMB Builds on Cyber Reskilling Lessons in Data Science Training Pilot.” Federal News Network, August 5, 2020. https://federalnewsnetwork.com/workforce/2020/08/omb-builds-on-cyber-reskilling-lessons-in-data-science-training-pilot-for-federal-workforce/.

[32] Ogrysko, Nicole. “With new CIO in place, OPM turning to familiar IT modernization playbook.” Federal News Network. August 31, 2021. https://federalnewsnetwork.com/technology-main/2021/08/with-new-cio-in-place-opm-turning-to-familiar-it-modernization-playbook/.

[33] “Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government,” National Archives. December 8, 2020. https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government.

[34] “California Consumer Privacy Act.” Office of the Attorney General. Accessed October 27, 2021. https://oag.ca.gov/privacy/ccpa.

[35] Newell, Rachel, Catherine Meyer, Meighan O'Reardon, and Deborah Thoren-Peden. “Virginia's Consumer Data Protection Act & CCPA-like State Privacy Laws.” Pillsbury Law, January 1, 1970. https://www.pillsburylaw.com/en/news-and-insights/virginia-consumer-data-protection-act-ccpa-state-privacy-laws.html#:~:text=The%20Virginia%20Consumer%20Data%20Protection%20Act%20%28CDPA%29%20was,to%20control%20how%20companies%20use%20individuals%E2%80%99%20personal%20data.

[36] HIPPA Journal. “Colorado Privacy Act Passed and Signed into Law.” HIPPAjournal.com. July 14, 2021. https://www.hipaajournal.com/colorado-privacy-act/#:~:text=The%20Colorado%20Privacy%20Act%20gives%20Colorado%20resident%20consumers,decisions%20that%20produce%20legal%20or%20similarly%20significant%20effects.

[37] Davis, Wright.“Baltimore City’s Ban on Facial Recognition Now in Effect,” Tremaine LLP, September 8, 2021, https://www.dwt.com/blogs/privacy--security-law-blog/2021/09/baltimore-facial-recognition-ban.

[38] “13 Cities Where Police Are Banned From Using Facial Recognition Tech,” Innovation & Tech Today, November 18, 2020, https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech/.

[39] “2020 IL H 53.” Illinois.gov. July 9, 2021. https://custom.statenet.com/public/resources.cgi?id=ID:bill:IL2021000H53&ciq=ncsl&client_md=cf812e17e7ae023eba694938c9628eea&mode=current_text.

[40] “Legislation Related to Artificial Intelligence.” NCSL, 2020. https://www.ncsl.org/rese arch/telecommunications-and-information-technology/2020-legislation-related-to-artificial-intelligence.aspx

[41] “Facial Recognition Gaining Measured Acceptance,” NSCL, September 18. 2020, https://www.ncsl.org/research/telecommunications-and-information-technology/facial-recognition-gaining-measured-acceptance-magazine2020.aspx.

[42] "What is VCSA?”, VCSA Cyber Skills Academies, accessed October 27, 2021, https://www.vacyberskills.com/.

[43] "Cyber Workforce Academy Maryland”, SANS, Accessed October 27, 2021, https://www.sans.org/about/academies/cyber-workforce-academy-maryland/.

[44] Passow, Amy. “How K-12 Schools Have Adopted Artificial Intelligence.” EdTech. January 3, 2019. https://edtechmagazine.com/k12/article/2019/01/how-k-12-schools-have-adopted-artificial-intelligence.

[45] “CISA Global,” Cybersecurity and Infrastructure Security Agency, February 2021, https://www.cisa.gov/sites/default/files/publications/CISA%20Global_2.1.21_508.pdf.

[46] “Strengthening international cooperation on artificial intelligence,” Brookings Institute, February 17, 2021, https://www.brookings.edu/research/strengthening-international-cooperation-on-artificial-intelligence/.

[47] “EU-US: A new transatlantic agenda for global change,” European Commission, December 2, 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2279.