

**SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION:  
QUESTIONS FOR THE RECORD**

**NOMINATIONS HEARING  
JULY 24, 2019**

**Written Questions Submitted to Michael Kratsios, Nominee to be Associate Director of the  
Office of Science and Technology Policy**

*Submitted by Senator Moran*

*Question 1.* Senator Udall and I led the enactment of the Modernizing Government Technology (MGT) Act in 2017 in an effort to replace unsupported, legacy IT systems that plague federal agencies and pose significant cybersecurity risks to the nation's critical infrastructure. While individual federal agencies need to remain vigilant in identifying and replacing their legacy IT systems, what role does the White House Office of Science and Technology Policy play in coordinating such efforts across the federal government?

Outside replacing legacy IT systems, do you have other suggestions for this Committee as to what should be done to improve the federal government's protections against cyber-attacks?

**Response:** *Upgrading the Federal IT infrastructure is of paramount importance. At the onset of this administration, the President created the American Technology Council with the stated intent of driving the modernization of Federal IT. Both the OSTP Director and U.S. CTO are members of this council, and if confirmed, I will use the ATC as a venue for ensuring that federal agencies maximize use of the important tools which Congress has provided to undertake this important effort. On behalf of the ATC, my office coordinated a report to the President on Federal IT Modernization. This report laid out over 50 actions that Federal Agencies needed to perform to jumpstart their IT Modernization efforts to improve their cybersecurity posture, and all of these actions have been completed. These actions, combined with important legislation such as the MGT act, have set the stage for Federal Agencies to greatly improve their cybersecurity posture through IT Modernization.*

*In addition, OSTP plays an important role in coordinating the research and development (R&D) needed to address longer term cybersecurity challenges and risks to the nation's critical infrastructure. Through the Networking and Information Technology Research and Development (NITRD) Program, OSTP is developing a Strategic Plan Implementation Roadmap to coordinate cybersecurity R&D efforts across the federal government. This Strategic Plan Implementation Roadmap is being prepared per statutory requirement for public provision of this information pursuant to the Cybersecurity Enhancement Act of 2014, Public Law 113-274, Section 201(a)(2)(D), Implementation Roadmap, and under direction from the NITRD*

*Subcommittee of the National Science and Technology Council Committee on Science and Technology Enterprise.*

*This Implementation Roadmap will provide information on the projects and programs being planned or carried out in fiscal years 2019, 2020, and possibly beyond, to meet the objectives of the 2016 Federal Cybersecurity Research and Development Strategic Plan, which was developed by NITRD's Cyber Security and Information Security and Assurance Interagency Working Group. The strategic plan provides priorities for cybersecurity R&D in alignment with the NIST Framework for Improving Critical Infrastructure Cybersecurity, which provides guidance on managing and reducing cybersecurity risk confronted by businesses and organizations.*

*Question 2. Earlier this month, OMB released a request for information to identify access or quality improvements for federal data sets and models. Given the Administration's commitment to boosting research initiatives around artificial intelligence demonstrated by announcements like the American AI Initiative, what type of feedback is the Administration seeking in this request for information? Are there plans going forward beyond collecting this information?*

**Response:** *As called for by the American AI Initiative, this OMB request for information (RFI) invites the public, the research community, and the private sector to identify improvements to Federal data and models needed to accelerate innovative, trustworthy AI. This RFI will help guide the efforts of agencies in identifying opportunities to increase data and model access and use by the greater non-Federal AI research community in a manner that benefits that community, while protecting safety, security, privacy, and confidentiality. The availability of these data sets and models to the AI R&D community could stimulate new developments that would enhance the transparency and explainability of AI applications, as well as illuminate ways to ensure the robustness, security and safety of AI applications.*

*In identifying data and models for consideration for increased public access, agencies will identify any barriers to, or requirements associated with, increased access to and use of such data and models, including privacy and civil liberty protections, safety and security concerns, data documentation and formatting, and any other changes necessary to ensure appropriate data and system governance.*

*Agencies will identify opportunities to use new technologies and best practices to increase access to and usability of open data and models, and explore appropriate controls on access to sensitive or restricted data and models, consistent with applicable laws and policies, privacy and confidentiality protections, and civil liberty protections.*

*Agencies will also be requested to improve data and model inventory documentation to enable discovery and usability, and to prioritize improvements to access and quality of AI data and models based on the AI research community's user feedback.*