FOR IMMEDIATE RELEASE
January 22, 2024
https://bis.doc.gov

BUREAU OF INDUSTRY AND SECURITY
Office of Congressional and Public Affairs
OCPA@bis.doc.gov

BIS ANNOUNCES APPOINTMENT OF ELIZABETH "LIZ" CANNON AS EXECUTIVE DIRECTOR OF OFFICE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY AND SERVICES

WASHINGTON, D.C. – The U.S. Department of Commerce's Bureau of Industry and Security (BIS) announced today that Elizabeth "Liz" Cannon will serve as the first Executive Director of the Office of Information and Communications Technology and Services (OICTS) beginning on Monday, January 22, 2024. OICTS is responsible for implementing the Information and Communications Technology and Services (ICTS) Program for the Department of Commerce.

"Liz brings extensive national security experience from both government and the private sector," said **Under Secretary of Commerce for Industry and Security Alan Estevez**. "I am thrilled about her addition to the BIS team and the leadership she will bring to OICTS."

In this role, Liz will manage policy developments and operations for OICTS. "I feel very fortunate to be the first Executive Director of the ICTS program," Liz said. "I look forward to safeguarding our nation's information and communications systems from foreign adversaries through an open and collaborative process."

Liz joins BIS from Microsoft, where she served as Senior Corporate Counsel for Global Trade. In that capacity, she was responsible for monitoring export controls, sanctions, and other international trade and security policy issues. She also oversaw Microsoft's Risk Intelligence Group, which conducts due diligence and trade-related investigations.

Liz also brings more than a decade of public service and national security experience from the Department of Justice (DOJ), including five years as Deputy Chief for Export Controls and Sanctions in the National Security Division. In this role, she supervised all criminal cases involving export control and sanction violations around the country. During her service at DOJ, she prosecuted national security cases including: espionage, economic espionage, mishandling of classified information, cyber offenses, and sanctions and export control offenses. She also spent time in private practice at an international law firm.

She holds a Bachelor of Science in Commerce from the University of Virginia and a Juris Doctorate from New York University School of Law.

About the Office of Information and Communications Technology and Services:

The ICTS program became a mission of BIS in 2022. OICTS is charged with implementing a series of Executive Orders (EOs), under the International Emergency Economic Powers Act,

focused on protecting domestic information and communications systems from threats posed by foreign adversaries. The ICTS program authorities include:

1. EO 13873 – "Securing the Information and Communications Technology and Services Supply Chain" (May 15, 2019), delegates to the Secretary of Commerce broad authority to prohibit or impose mitigation measures on any ICTS Transaction, subject to United States' jurisdiction, that poses undue or unacceptable risks to the United States.
2. 15 C.F.R. Part 7 – "Securing the Information and Communications Technology and Services Supply Chain," encompasses the implementing regulations for the OICTS program, mainly by establishing the scope of an ICTS Transaction and creating a process for investigating and reviewing ICTS Transactions; that the Department or other agencies (through referrals) believe may pose an undue or unacceptable risk. Ultimately, the Secretary can prohibit or mitigate ICTS Transactions if those transactions pose one of the three risks outlined in EO 13873.
3. EO 13984 – "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities" (January 19, 2021), directs the Secretary of Commerce to propose rules to address malicious cyber actors' use of Infrastructure as a Service (IaaS) by proposing "Know-Your-Customer" requirements.
4. EO 14034 – "Protecting Americans' Sensitive Data from Foreign Adversaries" (June 11, 2021), builds upon EO 13873 to address threats posed by "connected software applications" linked to foreign adversaries.
5. EO 14110 – "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" (October 30, 2023), builds on EO 13984, directing the Secretary of Commerce to impose record keeping requirements on IaaS providers when transacting with a foreign person to train certain large artificial intelligence models.