

Mark Bristow

Mark Bristow is the Branch Chief for Cyber Defense Coordination within Threat Hunting subdivision in the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS). He oversees DHS's efforts for assisting asset owners to respond to, remediate and recover from cyber incidents across government, critical infrastructure and private sector systems—most recently including securing the election infrastructure and addressing Russian attempts to gain access to the U.S. power grid.

Mr. Bristow joined DHS in 2008, working as a contract Incident Responder and then was promoted to Chief, Incident Response and Management for the Industrial Control Systems Cyber Emergency Response team (ICS-CERT). Mark later served as Deputy Director and then Director of the NCCIC Hunt and Incident Response Team (HIRT). He has prior experience conducting ICS assessments and penetration tests in multiple sectors with a focus on electric power generation, transmission and distribution.

Mr. Bristow brings a wealth of information security expertise and passion for solving the most complex problems to the Department. In his 12-year security career, he also has worked in the security industry where he supported a variety of private and public sector clients. Additionally, he teaches students and shares real-world experiences to help others learn to protect critical infrastructure. Having found his first bug in an ICS system at the young age of 10, Mr. Bristow has successfully blended his professional and personal goals to positively impact the cybersecurity community.

Mr. Bristow holds a bachelor's degree in Computer Engineering from Pennsylvania State University. He is a certified SANS instructor and holds CISSP, GCIH, GRID and GICSP certifications.