Immigration and Customs Enforcement (ICE)

Immigration and Customs Enforcement (ICE) - Homeland Security Investigation (HSI)

The ICE Homeland Security Investigations (HSI) directorate is a critical asset in the ICE mission, responsible for investigating a wide range of domestic and international activities arising from the illegal movement of people and goods into, within and out of the United States. HSI investigates immigration crime, human rights violations and human smuggling, smuggling of narcotics, weapons and other types of contraband, financial crimes, cybercrime, and export enforcement issues. ICE special agents conduct investigations aimed at protecting critical infrastructure industries that are vulnerable to sabotage, attack or exploitation. In addition to ICE criminal investigations, HSI oversees the agency's international affairs operations and intelligence functions. HSI consists of more than 10,000 employees, consisting of 6,700 special agents, who are assigned to more than 200 cities throughout the U.S. and 47 countries around the world. More information on ICE/HSI can be found by visiting http://www.ice.gov/about/offices/homeland-security-investigations/.

ICE HSI is especially interested in students who have completed coursework or previous work assignments related to: forensic analysis, network monitoring/network defense, hardware, basic programing and cybersecurity research and technical writing.

Immigration and Customs Enforcement (ICE)-Office of Chief Information Officer (OCIO)

ICE OCIO delivers innovative information technology and business solutions that enable ICE to protect and secure our nation to be the premier IT organization in the federal government recognized for how our people, processes and technologies create a secure and confident America.

ICE OCIO is especially interested in students who have completed coursework or previous work assignments related to: cyber security tools and capabilities, threat analysis, cybersecurity research and technical writing, and basic knowledge and understanding of industry best practices regarding policies, governance, strategies and standards in cybersecurity; and testing and development.