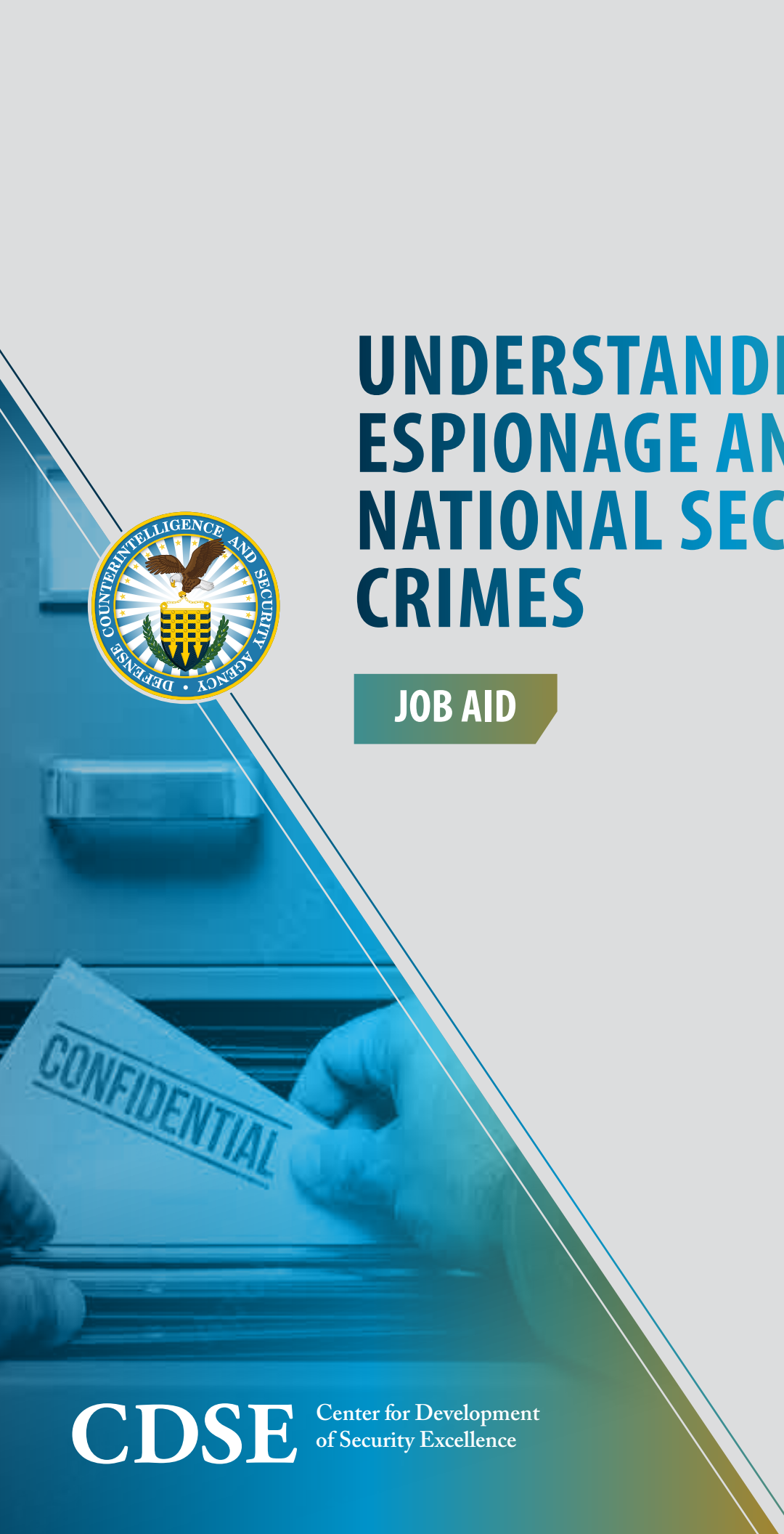
NOVEMBER
2024

UNDERSTANDING ESPIONAGE AND NATIONAL SECURITY CRIMES

JOB AID



CDSE Center for Development of Security Excellence

U.S. defense information comprises more than just classified information. Targeting of defense information has included dual-use technology, military critical technology, sensitive company documents, proprietary information, and Export Administration Regulation (EAR) or International Traffic in Arms Regulation (ITAR) controlled technology.

THIS CAN BE CONFUSING

If we are talking about counterintelligence and countering espionage, what does this have to do with sensitive company documents?

ESPIONAGE

Espionage is a national security crime; specifically, it violates **Title 18 USC, §§ 792-798** and **Article 106a, Uniform Code of Military Justice** (UCMJ). Espionage convictions require the transmittal of national defense information with intent to aid a foreign power or harm the U.S. However, even gathering, collecting, or losing national defense information can be prosecuted under Title 18.

ECONOMIC ESPIONAGE

Up until the passage of the **Economic Espionage Act of 1996**, many people used the phrases "Economic Espionage" and "Trade Secret Theft" interchangeably. Many people actually still do, but there is a difference. Economic Espionage is defined under §1831 of the Act and comprises behavior that denies the rightful owner of the economic benefit of property that the owner has gone to reasonable means to protect and does so with the intent to benefit a foreign entity.

TRADE SECRET THEFT

Trade Secret Theft is defined under **§1832 of the Economic Espionage Act of 1996** and covers the conversion of a trade secret to the economic benefit of anyone other than the rightful owner. There is no requirement for a foreign nexus in Trade Secret Theft.

ITAR/EAR VIOLATIONS

ITAR and EAR are export control laws whose broad scope extends to products, software, technical details, and services, and includes both military and commercial items.

WHICH ONES APPLY TO ME?

As DOD security professionals, which of these do you think you need to be worried about? In fact, all of these are relevant. Traditional Espionage may be the most obvious, but Economic Espionage also involves the loss of U.S. information to a foreign entity. Trade secret theft involving information related to a technology or security program, even if the information stops short of being classified, could provide critical information about your program, your personnel, or an emerging technology.

Remember, we can't always accurately determine the end user. What appears to be a domestic perpetrator may in fact turn out to be a foreign collection effort. ITAR and EAR Violations are criminal acts that must be reported. Though these different violations may result in different courses of action against the perpetrators, suspected violations of any of these laws must be reported to your security officer and/or the appropriate federal agency. For more information on reporting visit, the CDSE website and enroll in our **Counterintelligence Awareness and Reporting Course for DOD Employees**.