The Treasury Department also oversees some export laws. The Office of Foreign Assets Control (OFAC) enforces trade sanctions and embargoes. It is part of the Treasury Department. The OFAC administers trade sanctions and embargoes as part of United States foreign policy goals. It has the power to forbid some types of transactions based upon these goals. You can learn about the OFAC's sanctions programs at *http://www.treasury.gov/resource-center/sanctions/Pages/default.aspx.*

OFAC regulations may forbid people in the United States from engaging in any trade or financial transactions with other countries. People in the United States are prohibited from engaging in trade with certain people in other countries. For example, the government prohibits trade with known terrorists or drug traffickers.

The OFAC publishes a list of individuals and companies that people in the United States are generally forbidden from dealing with. The people on this list are called *specially designated nationals (SDN)*. You can view the OFAC's SDN list at *http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx.*

Penalties for violating OFAC regulations are generally the same as for EAR violations.

Case Studies and Examples

The following case studies and examples show how the concepts discussed in this chapter are used. These case studies are real-world examples of information security issues in the federal government.

Missing Hard Drives

In March 2009, the National Archives and Records Administration (NARA) learned that an external hard drive was missing. The hard drive held data from President William Clinton's administration. The data included the personal information of people who visited or worked at the White House during this time. The hard drive held two terabytes of data.

NARA discovered that the hard drive was missing on about March 24, 2009. On April 2, 2009, NARA notified its Inspector General that the hard drive was missing. It also reported it to US-CERT. NARA's Inspector General, the U.S. Secret Service, and the FBI are investigating the missing hard drive. It's not known if the hard drive was misplaced or stolen. NARA has offered an award of up to $50,000 for information about the case.

NARA had a backup copy of the hard drive. The NARA IG analyzed the hard drive. The IG determined that the hard drive held personal data. The IG also said that NARA needed to notify the people whose personal information was on the hard drive. As of January 4, 2010, NARA had notified over 175,000 people about the potential breach. You can read a NARA fact sheet about the breach at *http://www.archives.gov/press/press-releases/2010/pdf/nara-breach-notification-faq-2010-01-12.pdf.*

Social Networking Sites

The military must balance competing interests when thinking about information security. Most important, the DoD must make sure that it protects the lives of service members. In early 2010, the DoD issued a policy on using social media sites. Social media sites can be a potential danger. This is because of the amount of data that people sometimes post on these sites. Information posted on a social networking site could disclose where troops are stationed. The sites also are important ways for troops to communicate with family members.

In its policy, the DoD recognized that the Internet is critical to its operations. It helps people stay connected. The Internet also helps the DoD advertise the services that it provides to the country. The policy allows DoD employees to use its non-classified Internet system to access social media sites such as Facebook and Twitter. The policy also allows DoD components to maintain official DoD communications on social media sites. The DoD component must receive approval to do this.

This policy was updated in 2012 to more clearly state that DoD doesn't stop its employees from using social media from their personal devices for personal purposes. You can read the policy at *https://www.slideshare.net/DepartmentofDefense/dtm-09-026*.

CHAPTER SUMMARY

This chapter reviews the laws that protect the security and privacy of data that the federal government uses. FISMA is the main law protecting the security of federal government IT systems. It requires federal agencies to create information security programs. Agencies also must review their information security risks. The law requires them to implement controls to mitigate those risks.

The Privacy Act of 1974 and the E-Government Act of 2002 are the main laws protecting data privacy at the federal level. These laws govern how federal agencies use personally identifiable data. Under the E-Government Act, federal agencies must review their IT systems for any privacy impacts. Both laws require federal agencies to notify the public about their data collection practices.