Foreign adversaries and competitors are actively seeking information that is vital to our national and economic security, U.S. global competitiveness, and your organization’s mission. This includes:

- Sensitive or proprietary financial, trade, or economic policy information
- Pioneering research and development
- Emerging technologies
- Sector-specific information, including commerce, transportation, agriculture, health, homeland security, energy, and communications

The National Counterintelligence and Security Center (NCSC)
is the nation’s premier source for counterintelligence and security expertise, and a trusted mission partner in protecting America against foreign and other adversarial threats.

**THEIR METHODS**

- **Elicitation** — Use of conversation to extract information, either in person, by email, on the phone, or through social media.
- **Social Engineering** — The impersonation of others to seem legitimate and surreptitiously acquire passwords or other key data.
- **Economic Espionage** — The theft or misappropriation of a trade secret with the intent or knowledge that the offense will benefit a foreign entity.
- **Human Targeting** — The targeting of individuals with access to sensitive information, who, for example, might unexpectedly meet someone who shares their interests or seeks an ongoing relationship.
- **Cyber/Technical** — Digital technologies used to compromise or acquire information stored or transmitted electronically.

**PROTECTING YOUR ORGANIZATION’S SECRETS**

Safeguarding Sensitive and Proprietary Information from Foreign Adversaries and Competitors
You may be a target. And in this fight, you matter.

You have access to facilities and computer networks, as well as sensitive information, resources, technologies, research and other data that our foreign adversaries and competitors desperately want.

Our adversaries and competitors are interested in you because you have connections and access.

You also have social media accounts. A work and/or personal smartphone. Social and professional networks include others in sensitive positions. You may travel, both domestically and abroad.

These are all potential vulnerabilities.

YOUR EMAIL

Phishing is a common method used to compromise computer networks and gain access to valuable information they contain. You may receive a seemingly real and plausible or official-looking email, text message, or pop-up window to lure you into clicking on a link or attachment. That action allows the attacker to bypass your network’s technical defense, upload malware, or otherwise infiltrate your network and steal information.

▶ Never click on suspicious links or attachments.

YOUR SOCIAL MEDIA

Social media provides adversaries and competitors with a platform to gain your trust. Attackers may create a fake profile to befriend or follow you, posing as a former acquaintance, a job recruiter, or someone with a shared interest, trying to deceive you into revealing more information about yourself or your work.

▶ Maximize your privacy settings on social media, and use caution with what you share.

YOUR TRAVEL

Never assume you have any electronic privacy when traveling abroad. Internet cafés, hotel business centers, hotel WiFi networks, and even charging stations at international airports can provide points-of-access into your devices, and thereby, your communications. Always take your electronics with you (a hotel room safe isn’t really “safe”), and always be mindful about whether you truly have a secure connection.

▶ When abroad, have no expectation of privacy.