SAFETY AND SECURITY

Cybersection

10 Things to Know About Personally Identifiable Information (PII)

For years, the department has recognized the importance of protecting assets from criminals who hack into computer systems over the internet.

“Awareness of cybersecurity has grown as more people and companies have identified this issue as a top priority,” said Secretary Robin L. Wiessmann. “What everyone needs to recognize is that Personally Identifiable Information is at least as valuable as money. People should be treating their information the same way they treat their money.”

Wiessmann points to **10** examples of PII that everyone should guard:

1. Social Security number, full and truncated;
2. Driver’s license and other government identification numbers;
3. Citizenship, legal status, gender, race/ethnicity;
4. Birth date, place of birth;
5. Home and personal cell telephone numbers;
6. Personal email address, mailing and home address;
7. Mother’s middle and maiden names;
8. Spouse information, marital status, child information, emergency contact information;
9. Financial information, medical information, disability information;
10. Law enforcement information, employment information, educational information.

The Federal Trade Commission has published a guide for businesses on protecting PII.

Free Cybersecurity Assessments, Services Available

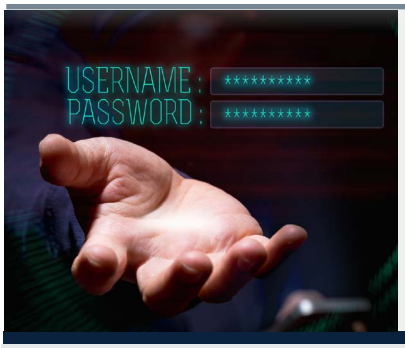
As part of its National Cybersecurity and Communications Integration Center (**NCCIC**), the U.S. Department of Homeland Security offers several cybersecurity assessment services through its **National Cybersecurity Assessments and Technical Services (NCATS) program**.

NCATS offers cybersecurity services to federal agencies, state and local governments, critical infrastructure, and private organizations at no cost. The core capabilities are:

- **Vulnerability Scanning**
- **Risk and Vulnerability Assessments**
- **Remote Penetration Testing**
- **Validated Architecture Design Review**

The program conducted more than 160 on-site enterprise and control systems assessments in fiscal year 2017. NCATS works with a public or private organization to help it uncover its cybersecurity deficiencies and how it may overcome any weaknesses. Following the assessment, they issue a detailed report outlining vulnerabilities and suggested steps to help mitigate any flaws.

For more information on any of these services, contact 888.282.0870 or **ncciccustomerservice@hq.dhs.gov**.



Position Issued on Use of Investor Client Usernames, Passwords

The department’s Bureau of Securities Compliance and Examinations has issued a position on the use of client usernames and/or passwords by registered investment advisors and investment advisor representatives.

The Bureau considers registrants’ use of client usernames and/or passwords to access client custodial accounts as a dishonest and unethical practice. Read more about the Bureau’s position and remedial actions to be taken **here**.