INSIDER THREAT AWARENESS

"Insider threat" is the term used for the potential harm that may result from an authorized user intentionally or unintentionally using their access to negatively affect information or systems, and ultimately compromising University goals and the mission of our research sponsors.

Insiders committing illegal acts and unauthorized disclosures can negatively affect national security and U.S. industry in many ways, for example:

- loss of intellectual property rights which could in turn lead to loss of
  - technological advantage
  - revenue
- compromise of classified or controlled unclassified information (CUI), e.g., export-controlled, proprietary, financial, or private information
- economic loss
- physical harm or loss of life

Insiders have arguably caused more damage to the security of the United States than foreign intelligence officers. Insiders are often more aware of vulnerabilities they can exploit to their benefit than outsiders, and, with today's technologies, have the ability to cause more harm than before. What used to take years to collect now takes minutes because of the increased use of removable media. This document is aimed at increasing awareness of insider threats an overview of the types of insider threats, as well as behaviors and other signs which may point to the existence of an insider threat. Procedures and contact information for reporting suspected threats will also be highlighted.

LOOK FOR AND REPORT INDICATORS OF POSSIBLE INSIDER THREATS

It's important for everyone to apply appropriate safeguards to protect information subject to access or dissemination restrictions (e.g., proprietary, export-controlled, classified or controlled unclassified information), but that alone is not sufficient. It is also important to be alert for signs or behaviors that might indicate an insider threat:

- mishandling or misuse of University or sponsor information
- removal of University or sponsor information from premises for unauthorized, personal, or unknown reasons
- unauthorized or unnecessary duplication of University or sponsor CUI
- engaging in conversations involving or about non-public technical information without a need-to-know
- establishment of unauthorized methods of access to University or sponsor information systems
- non-job-related requests for access to University proprietary, controlled sensitive, or classified information
- unreported foreign contracts or overseas travel
- sudden reversal of financial situation or repayment of large debts or loans

A variety of more personal circumstances or behaviors, such as the examples below, may also indicate increased potential for insider threats:

- depression
- stress in personal life
- exploitable behavior traits such as alcohol/drug use or gambling
- financial trouble
- prior or current disciplinary issues

Not all suspicious behaviors or circumstances indicate a threat; ultimately each situation must be evaluated along with relevant evidence to determine whether a true insider threat exists that must be addressed. However, it is essential to report any suspicious behaviors that may point to a threat. Observing even a single activity and not reporting it can increase the likelihood and extent of damage due to an insider threat. Also, particularly in the case of personal circumstance or behavior changes, not reporting the observation may represent a lost opportunity to help a colleague who may be struggling.

How Do I Report Suspicious Behavior?

It is important to avoid confronting the individual directly. If you observe any of these suspicious behaviors by an individual or group of individuals, please report the activity to your supervisor, Export Controls, Information Security, or, if you're a cleared employee, to the Facility Security Officer.

Case Example: Go with your Gut

Ana Belen Montes was recruited by Cuba after learning of her views against the U.S. policies towards Central America. At that time, she was a clerical worker in the Dept. of Justice. She went to work for the Defense Intelligence Agency and became the DIA's top Cuban analyst.

While security officials became aware of her disagreement with U.S. foreign policy and had concerns about her access to sensitive information, she had passed a polygraph test.

According to a FBI news story, in 1996 "an astute DIA colleague – acting on a gut feeling – reported to a security official that he felt Montes might be under the influence of Cuban intelligence." She was interviewed, but admitted nothing.

Four years later when the FBI was working to uncover an unidentified Cuban agent, the security official recalled the interview and contacted the FBI. An investigation was opened that led to her arrest and conviction.

THREAT LANDSCAPE

Institutions of higher education are a target for foreign intelligence and intellectual property collectors attempting to gain military and economic advantages. It's important to remember that you may not be the ultimate target but rather a single link in the chain to get the adversary to the information they seek, which may belong to the University, a sponsor, or a collaborator. They may also simply be looking to build connections and relationships now that they can capitalize on in the future.

Current technologies and easily accessible information about businesses and people enable social engineering attacks that vary greatly in their level of sophistication.

Adversary Method: Spear Phishing

Spear phishing attacks use social engineering to trick an individual into providing information or clicking on a link or attachment containing malicious software that can provide unauthorized network access, ex-filtrate information, or do other harm. It is called *Spear* phishing because the emails appear to come from people you know or about events you are familiar with, such as an upcoming conference or request for an article re-print. You should become familiar with ways to detect phishing emails by reviewing the Information Security's Phishing website at: http://www.secureuva.virginia.edu/phishing/.

When in doubt about whether an email is phishing or not, contact the sender via a method NOT described in the email. For example, if it appears to come from a colleague, do not email them, call them (because sometimes the attackers take over your colleagues email account and reply to emails about whether the email sent is legitimate!)

Also be suspicious of unsolicited or unusual requests via voicemail, phone calls, or text messages. All of these have been used to trick individuals into providing information or unknowingly installed malicious software.

How Do I Report Suspicious Behavior?

Report spear phishing and other suspicious activities, for example anomalous computer behavior, to Information Security at abuse@virginia.edu.

Adversary Method: Elicitation

Elicitation is the strategic use of conversation to subtly extract information about you, your work, or your colleagues. Foreign intelligence officers are trained in elicitation tactics. When done well, elicitation is perceived by the target as harmless small talk.

The internet and social networking sites make it easy to obtain public information to create plausible cover stories to begin friendships with persons who have access to University CUI or classified information. Using social media and other public resources, an individual seeking to do harm may initiate a conversation or relationship that seems benign initially, enabling him or her to gradually elicit information that the foreign operative can then use to invoke harm. Unsolicited requests to review thesis papers, draft publications, or other research-related documents outside of normal professional activities (e.g., sponsor or journal peer review requests and consulting agreements); requests from unknown parties to serve on a dissertation or thesis committee; or unsolicited invitations to attend international conferences may also be elicitation attempts. One should never reply to unsolicited requests for information other than to provide copies of or links to information that is in the public domain.

Individuals should always be aware of the possibility of elicitation attempts at work, while attending trade shows or conferences, and in casual settings. It is essential to know what information cannot be shared and to be suspicious of those who seek that information. Possible responses to someone who is attempting to elicit information include referring them to the internet, changing the topic, or providing a vague answer.

How Do I Report Suspicious Behavior?

It is important to avoid confronting the individual directly. Also, elicitation is subtle and can be difficult to recognize. Therefore, suspicious emails should be reported to Information Security (abuse@virginia.edu). Reports of suspicious behaviors or other activities can be made by phone or in person to Export Controls or, if you're a cleared employee, to the Facility Security Officer.

Adversary Method: Recruitment

Recruitment is the process of obtaining cooperation from someone to provide information. Anyone with access to University CUI or classified information could be a potential target. It is important to safeguard actions and words to avoid becoming an easy target.

Targets may not realize at first that they have been identified for possible recruitment. Initial interactions with the adversary will typically involve attempts to determine levels and types of current or future information access, and whether or not the information is of value.

If the adversary is interested, he or she will attempt to develop the relationship and devise a ruse to establish a logical basis for continuing contact. The adversary will continue to assess the target's willingness to provide information.

The adversary's goal is to establish a relationship based upon trust. Early requests may seek to establish trust through solicitations for professional advice or information about a co-worker. Targets often feel obligated to reply or will provide information because they are flattered by this level of trust. The adversary could then heighten the sensitivity level of the requests commensurate with the deeper trust level of the relationship.

Unsolicited gifts, in the form of funding or research equipment, particularly from entities you haven't worked with before, may also represent the start of a recruitment attempt.

How Do I Report Suspicious Behavior?

It is important to avoid confronting the individual directly. You are not being asked to avoid or report all contacts, but if you suspect you're being recruited, report the situation to Export Controls or, if you're a cleared employee, the Facility Security Officer.

> ***Case Example: As Much Time as It Takes***
>
> *In 2010, ten deep-cover Russian spies were arrested. The individuals in the group married, bought homes, and had children as they appeared to assimilate into American life while actively collecting information and spotting and assessing potential recruits.*

IF YOU SEE SOMETHING, SAY SOMETHING!

The goal of reporting unusual activities is not to act as a "snitch" or embarrass another person. Rather, it is to prevent loss, reduce impact, and mitigate damage. After all, no one wants to look back at the extent of the damage that could have been prevented had they simply reported a suspicious behavior. Ongoing compliance with security requirements is everyone's responsibility and needs to be taken

seriously. Other than implementing and following appropriate safeguarding procedures, reporting suspicious behaviors or contacts is the most important thing you can do to support compliance objectives.

Threats and security compromises related to cyber security should be reported directly to Information Security at abuse@virginia.edu. Call 911 to report immediate threats to personal safety or physical security. Non-emergency situations can be reported by calling the UVA police department at 434-924-7166.

University employees, students, and fellows are encouraged to report through institutional channels prior to contacting a state or federal hotline and are strongly advised against directly confronting the individual or group of individuals involved. However, if you are not satisfied with the results of your contact at the University level, you are encouraged to report to the applicable state or federal hotline. Comments and questions made during these contacts must be kept unclassified and should not disclose CUI.

CONTACT INFORMATION FOR QUESTIONS ABOUT INSIDER THREATS

If you have questions now or in the future about Insider Threats, please reach out to a staff member with University Information Security (https://security.virginia.edu/about-university-information-security), Export Controls (https://export.virginia.edu/contacts), or if you're a cleared employee the Facility Security Officer.

By signing below, I acknowledge I have reviewed and understood the material in this document and will follow its instructions to the best of my ability.

_____	_____
Signature	Date
_____	_____
Printed Name	Computing ID