Promoting Situational Awareness at Your University

FOR THE UNIVERSITY INDIVIDUAL

AWARENESS

- ☐ Determine what might make you a person of interest for intelligence collection
  - Expertise and research, or political endeavors
  - Privileged access to locations, items, data, and/or people
  - Knowledge of research activities, security protocols, networks, and/or sensitive personnel information
- ☐ Determine potential vulnerabilities
  - Excited and passionate about work, great desire to talk about it
  - Regularly contacted by unknown persons requesting insights, assistance, guidance
  - Collaborate frequently across a broad professional network
  - Routine travel to present work or conduct research
  - Frequently post on social media
  - Limited understanding of threats or disregard for operational security

PREVENTION

- ☐ Be mindful of requests for information or quickly developed relationships that seem a little "off"
- ☐ Be discrete with information shared, even if it seems trivial
- ☐ Avoid posting information that could be compromising
- ☐ Limit social media access to those you know
- ☐ Vet individuals soliciting connections into professional networking sites – do not accept individuals who have not contacted you otherwise, do not have shared expertise, or otherwise invitations seem "different"
- ☐ Carefully consider motives for gifts, honors, or unique opportunities
- ☐ Use strong passphrases/complex passwords for accounts and devices

TRAVEL-SPECIFIC

- ☐ Assume no data privacy while abroad; do not travel with patentable, proprietary, or otherwise sensitive material
- ☐ Secure your devices:
  - Travel with a "clean" laptop and use a "clean" phone (no photos, emails, banking apps, social media)
  - Update anti-virus software and establish firewalls; disable "remember me" functions
  - Turn off Wi-Fi functions when not using; do not use public/open Wi-Fi; determine if use of university VPN is legal in locations of travel
  - Do not download files, applications, software, etc.
  - Upon return from travel, have university IT scan devices scanned before connecting to any networks
- ☐ Minimize your digital footprint
- ☐ Do not access personal accounts
- ☐ Avoid discussing travel plans online, in public spaces, or while using public transportation
- ☐ Take steps to avoid having people in your lodging while you are gone
  - Keep the television or radio on to indicate you may be inside
  - Hang the "do not disturb" sign on your door…do not use housekeeping services
  - Do not use hotel safe

RESPONSE

- ☐ Share any concerns with someone **as soon as possible** (recommendations: Department Head, Travel Security, and/or Facility Security Officer)

FOR UNIVERSITY ADMINISTRATION

AWARENESS

- ☐ Determine potential persons of interest for intelligence collection across campus due to:
  - Expertise and Research or political endeavors
  - Access to locations, items, data, and/or people
  - Knowledge of research activities, security protocols, networks, and/or sensitive personnel information
- ☐ Determine potential organizational vulnerabilities
  - Physical security
  - Cybersecurity
  - Lack of clarity in institutional policies and/or inconsistent communication of them

PREVENTION

- ☐ Create cross-campus forums or working groups to discuss the threat
- ☐ Embed awareness into training
- ☐ Avoid posting information about researchers or research that could be compromising
- ☐ Proactively monitor university accounts and respond quickly to oddities
- ☐ Identify points of contact for individuals or departments to report concerns

TRAVEL-SPECIFIC

- ☐ Provide “clean” laptops for travelers at greater risk
- ☐ Provide pre-travel laptop hardening (updates to anti-virus and software and scan for malware) and post-travel “cleaning” to scan for malware
- ☐ Provide additional resources to travelers visiting countries where risk of compromise is greater

RESPONSE

- ☐ Share any concerns with someone **as soon as possible** (recommendations: Department Head, Travel Security, and/or Facility Security Officer