DEFENSE SECURITY SERVICE
TARGETING U.S. TECHNOLOGIES
SUMMARY OF FY17 INDUSTRY REPORTING

The *Summary of FY17 Industry Reporting* provides summary details of foreign intelligence entities' (FIE) targeting U.S. technologies as reported by cleared industry to the Defense Security Service during fiscal year 2017. This information sheet identifies the seven most commonly targeted technology categories of the Industrial Based Technology List, specific technology subcategories targeted, and FIE methodologies. This is a companion product to the annual Targeting U.S. Technologies report due out in September 2018, which will explore each technology in greater detail.

AERONAUTIC SYSTEMS

- **Most Reported Subcategories:** Unmanned Aerial Vehicles & Drones; Fixed Wing Combat Aircraft; Rotary Wing Aircraft
- **Primary Methods of Contact:** Email; Foreign Visit; Résumé – Academic
- **Primary Methods of Operation:** Request for Information/Solicitation; Attempted Acquisition of Technology; Exploitation of Business Activities
- **Top Regional Collectors:** East Asia & the Pacific; Near East; South & Central Asia

COMMMAND, CONTROL, COMMUNICATION, & COMPUTERS

- **Most Reported Subcategories:** Telecommunication Devices (phones, cell phones, radios, radio mounts); Antennas; Common Data Links
- **Primary Methods of Contact:** Email; Résumé – Professional; Résumé – Academic
- **Primary Methods of Operation:** Attempted Acquisition of Technology; Résumé Submission; Request for Information/Solicitation
- **Top Regional Collectors:** Near East; East Asia & the Pacific; South & Central Asia

ELECTRONICS

- **Most Reported Subcategories:** Circuit Boards; Integrated Circuits; Micro-sensors
- **Primary Methods of Contact:** Email; Résumé – Academic; Résumé – Professional
- **Primary Methods of Operation:** Attempted Acquisition of Technology; Résumé Submission; Request for Information/Solicitation
- **Top Regional Collectors:** East Asia & the Pacific; South & Central Asia; Near East

RADARS

- **Most Reported Subcategories:** Continuous Wave Radars; Electronically Steered Radars; Pulse Radars
- **Primary Methods of Contact:** Email; Résumé – Academic; Conferences, Conventions, or Tradeshows
- **Primary Methods of Operation:** Attempted Acquisition of Technology; Request for Information/Solicitation; Résumé Submission
- **Top Regional Collectors:** East Asia & the Pacific; South & Central Asia; Near East

ARMAMENT & SURVIVABILITY

- **Most Reported Subcategories:** Missiles; Body Armor; Armaments, Explosives, and Survivability
- **Primary Methods of Contact:** Email; Conferences, Conventions, or Tradeshows; Résumé – Academic
- **Primary Methods of Operation:** Request for Information/Solicitation; Attempted Acquisition of Technology; Résumé Submission
- **Top Regional Collectors:** East Asia & the Pacific; Near East; South & Central Asia

OPTICS

- **Most Reported Subcategories:** Optics; Lenses; Reflective Coatings
- **Primary Methods of Contact:** Email; Résumé – Academic; Web Form Submission
- **Primary Methods of Operation:** Attempted Acquisition of Technology; Request for Information/Solicitation; Résumé Submission
- **Top Regional Collectors:** East Asia & the Pacific; Near East; South & Central Asia

SOFTWARE

- **Most Reported Subcategories:** Modeling & Simulation Software; Software Algorithms; Artificial Intelligence Software
- **Primary Methods of Contact:** Email; Personal Contact; Résumé – Academic
- **Primary Methods of Operation:** Résumé Submission; Request for Information/Solicitation; Attempted Acquisition of Technology
- **Top Regional Collectors:** East Asia & the Pacific; Near East; Europe & Eurasia

DEFENSE SECURITY SERVICE
TARGETING U.S. TECHNOLOGIES
DEFINING THE TERMS

DSS counterintelligence analysts review each attempt to collect information related to U.S. technologies resident in cleared industry to identify the FIE's method of operation and method of contact. In an effort to provide greater understanding of the information on the other side of this page, we have included definitions for our methods below. They are listed alphabetical order.

METHODS OF OPERATION

Distinct patterns or methods of procedure thought to be characteristic of or habitually followed by an individual or organization involved in intelligence activity. These generally include attempts at:

Attempted Acquisition of Technology: Acquiring protected information in the form of controlled technologies, via direct contact or through the use of front companies or intermediaries, including the equipment itself or diagrams, schematics, plans, spec sheets, or the like.

Exploitation of Business Activities: Establishing a commercial relationship via joint ventures, partnerships, mergers and acquisitions, foreign military sales, or service provider; leveraging an existing commercial relationship in order to obtain access to personnel or protected information and technology.

Exploitation of Cyber Operations: Foreign intelligence entities or other adversaries compromising the confidentiality, integrity, or availability of targeted networks, applications, credentials or data with the intent to gain access to, manipulate, or exfiltrate personnel information or protected information and technology.

Exploitation of Experts: Gaining access to personnel or protected information and technology via requests for, or arrangement of, peer or scientific board review of academic papers or presentations; requesting a consult with faculty members or subject matter experts; or attempting to invite or otherwise entice subject matter experts to travel abroad or consult for foreign entities.

Exploitation of Insider Access: Trusted insiders exploiting their authorized placement and access within cleared industry or cause other harm to compromise personnel or protected information and technology.

Exploitation of Relationships: Leveraging existing personal or authorized relationships to gain access to protected information.

Exploitation of Security Protocols: Visitors or unauthorized individuals circumventing or disregarding security procedures or behaviors by cleared or otherwise authorized persons that indicate a risk to personnel or protected information and technology.

Exploitation of Supply Chain: Compromising the supply chain, which may include the introduction of counterfeit or malicious products or materials into the supply chain with the intent to gain unauthorized access to protected data, alter data, disrupt operations, or interrupt communication.

Résumé Submission: Foreign persons submitting résumés for academic or professional placement that would facilitate access to protected information to enable technological or economic advancements by the foreign entity.

Request for Information/Solicitation: Collecting protected information by directly or indirectly asking or eliciting personnel or protected information and technology.

Search/Seizure: Temporarily accessing, taking, or permanently dispossessing someone of property or restricting freedom of movement via tampering or physical searches of persons, environs, or property.

Surveillance: Systematically observing equipment, facilities, sites, or personnel associated with contracts via visual, aural, electronic, photographic, or other means to identify vulnerabilities or collect information.

Theft: Acquiring protected information with no pretense or plausibility of legitimate acquisition.

METHODS OF CONTACT

Approaches used to connect the foreign actor to the targeted individual, information, network, or technology in order for the foreign actor to execute the MO(s).

Conference, Conventions, or Tradeshows: Contact regarding or initiated during an event, such as a conference, convention, exhibitions, or tradeshow.

Cyber Operations: Activities taken directly against a targeted system; to include cyber network attack, cyber network exploitation, and collection.

Email: Unsolicited requests received via email for information or purchase requests.

Foreign Visit: Activities or contact occurring before, during, or after a visit to a contractor's facility.

Mail: Contact initiated via mail or post.

Personal Contact: Person-to-person contact via any means where the foreign actor, agent, or co-optee is in direct or indirect contact with the target.

Phishing Operation: Emails with embedded malicious content or attachments for the purpose of compromising a network to include but not limited to spear phishing, cloning, and whaling.

Résumé – Academic: Resume or CV submissions for academic purposes.

Résumé – Professional: Resume or CV submissions for professional purposes (e.g., seeking a position with a cleared company).

Social Networking Service: Contact initiated via a social or professional networking platform.

Web Form: Contact initiated via a company-hosted web submission form.

Telephone: Contact initiated via a phone call by an unknown or unidentified entity.