CYBER THREAT CASE EXAMPLES

- A defense contractor employee, working on military grade technologies for a cleared U.S. defense company, was contacted via email by a suspected representative of a foreign firm; however, it was noted that the requestor's firm's name did not match the incoming email address. The email correspondent claimed his firm had an "urgent requirement" for military-grade technology being developed at the contractor facility and wanted to establish a business relationship. Subsequent analysis revealed that the email address used by the correspondent was associated with a second foreign company having a history of end- user certificate fraud.

- A representative of a foreign research center contacted a cleared U.S. defense facility and subsequently provided product design schematics in an apparent attempt to justify obtaining export-controlled materials. A review of the schematics submitted by the foreign research center revealed that they were associated with a military critical technology program. At first, the foreign research center denied that the product in the schematics had any military applications, but when challenged, eventually recanted, admitting that the product design presented could indeed be used for military purposes. Despite this exposed deception, the foreign firm's representatives continued to maintain they had no intention of utilizing the final product for such purposes.

- A cleared U.S. defense company reported receiving multiple deceptive emails that (when opened) resulted in malicious software being automatically installed on the company's internal computer system. Numerous employees within this cleared defense company were victims of this ruse. Following the extraction and analysis of one of the malicious payloads, cleared U.S. defense analysts discovered additional malicious codes embedded in .gif and .jpg image files in the software.

- Over several months, a foreign firm repeatedly contacted an employee of a U.S. cleared defense company, cultivating his assistance in procuring components for the foreign firm's use. Although the contact had begun with a seemingly innocuous request for components that were not controlled, the foreign firm subsequently amended its list to include dual-use export controlled items. The foreign firm eventually shared the contractor employee's contact information with multiple sections inside the foreign firm, resulting in a flood of additional requests to the same contractor employee. Within a month, this same foreign firm shifted focus to a second employee within the defense company, requesting new technology known to be of interest to the military research and development efforts of the foreign firm's country of origin.

- An individual apparently posing as a foreign student contacted an employee working for a cleared U.S. defense company performing aerodynamics research, asking for what amounted to classified information on the cleared defense company's UAV applications. The foreign student, supposedly an aerodynamics major at a major foreign university, also inquired about the possibility of an intern position in the company's aerodynamics research branch. The "student's" requested information and research interests related to classified and export restricted technology known to be actively sought by the student's country of origin.

- An engineering team from a U.S. defense contractor participated in an approved exchange with a foreign counterpart team during which approved, unclassified technical information was commonly shared between participants. Following the exchange program’s completion, representatives of the U.S. company discovered several "export restricted" documents among a large volume of printed material left on-site by the foreign engineer team. Upon further review of the printed materials left by the foreign engineers, the U.S. company representatives discovered the foreign team had acquired a large amount of open source information on military programs clearly outside the scope of the unclassified contract with the cleared U.S. defense company.