# National Academies Security Roundtable

Joshua W. Massey

Director / ITPSO

Enterprise Risk Management

The MITRE Corporation



MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

# MITRE tackles complex challenges with no commercial interest.

Together with government and public private partnerships, we work to improve the safety, stability, and well-being of our nation.

We apply systems thinking to solve complex national and global problems, bringing an interdisciplinary perspective to R&D.

We operate six federally funded R&D centers, as well as MITRE Labs and an independent research program.


MITRE
SOLVING PROBLEMS FOR A SAFER WORLD®


MITRE

# Example of Illicit Elicitation:  Characteristics of Targeted

- **In March 2022, 57 MITRE employees were targeted by a foreign talent program recruitment campaign.**
- **Only 3 of the 57 employees who received the talent recruitment email reported it to MITRE security.**
  - Various reasons were given by employees who chose not to report the email, including assertions that they deleted it, ignored it, or never saw it.
  - While security professionals know that underreporting has always been an issue, a reporting rate of 5% in this case is far below expectations. Employees who did report the email noted that it was clear to them that the message and its sender were suspicious.
- **Greater employee awareness is important to improving reporting trends, which was demonstrated by a 39% increase in suspicious email reporting following an awareness campaign related to this incident.**
  - Improved reporting can alert security professionals to specific threats and broader risk trends, which provides corporate leaders with the necessary insight to adjust policies and risk mitigations, when needed.
  - Accordingly, education and training should emphasize not only the identification of suspicious contacts, but also the value and impact of self-reporting, like the discovery of broader campaigns and impact to organizational resilience and national security.

# Example of Illicit Elicitation:  Characteristics of Targeted

- **55 of the 57 employees that received the email were mid-career or senior management personnel,** which suggests that the foreign talent program desires participants who are experts in their field, senior enough to have substantial experience, but not too senior that they are no longer engaged in technical work. Although only two early career employees received the email, both were rising experts in Artificial Intelligence.
- **50 of the 57 employees had a Secret or Top Secret security clearance,** which suggests that the foreign talent program desires access to sensitive U.S. national security information.
- **At least 27 of the 57 employees were subject matter experts in Artificial Intelligence (25) or Quantum Information Technologies (2),** which the President's National Science and Technology Council (2022) identified as critical and emerging technologies. The prioritization of these critical technologies is in line with the objectives set forth in China's 14th Five-Year Plan (translated by CSET, 2021).
- **43 of the 57 were assigned to MITRE campus locations rather than smaller sites, although assigned location does not appear to be a factor in target selection.** The location breakdown of employee's who received the recruitment email track with broader MITRE location demographics (i.e., two-thirds of MITRE employees are assigned to campuses).

MITRE

# Example of Illicit Elicitation:  Characteristics of Targeter

- **Foreign Talent Program recruitment campaigns are often managed by ostensible "consulting" or "recruiting" companies.** The 2022 recruitment campaign played out over a period of fifteen days, during which point 57 unique employees receive an identical email from the same sender. The sender identified as a representative of a "consulting company that integrates the world's top talents," which matches a technique used in other talent recruitment campaigns targeting MITRE.
- **Chinese Talent Plans are likely adapting recruitment tradecraft due to increased awareness within the U.S. research community.** Increased vigilance by USG, industry security professionals, and members of the research community has resulted in greater awareness of the risk posed by these programs. As such, recruiters are likely adapting their methods to navigate improved security controls. For example, a Talent Program contract from 2018 identified the following operational security recommendations (OSTP, 2020, p. 29):

*In order to further do a better job in ensuring the safety/security of overseas talents, [we] ask the organizations not use e-mails in sending out notifications for interview/defense. Instead, they should use telephone calls or faxes in giving notifications in the name of inviting [the candidates] to come back to China to attend academic conferences and forums, the words "1000 Persons Plan" shall not appear in the written notifications.*

Joshua Massey
jwmassey@mitre.org
703-983-7553
Enterprise Risk Management (A220)

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™