Instructor Notes for the Identity Database Protection Scenario
February 2010

This scenario requires players to protect an identity database that is used in the generation of smart card IDs. The scenario does not address smart cards per se; rather it highlights some issues related to protecting a centralized database that is accessed by a variety of users. Security issues raised in this scenario include:

- Use of network filters and/or VPNs to protect information that must be accessed via the Internet;
- Use of background checks to reduce the risks of insider threats
- Use of operating system access control mechanisms to limit modes of access (e.g., read only rather than read-write).
- The risk of an enemy's use of inference to deduce information from accessible databases that lack suitable "cover stories" in place of redacted classified information.
- An attacker's motive to subvert databases that control smart card issuance is affected by the attacker's motive to compromise assets that are protected by the smart cards. For example, if a smart card controlled smart lock is deployed to protect a very high motive asset, then the attacker may apply that high motive toward compromising identity databases used in smart card creation.

Students are expected to have completed at least the "Filters" scenario, and probably the Introduction to VPNs scenario.

The scenario is not intended to simulate or represent any particular real-world system. Rather, it uses a hypothetical smart card generation process to illustrate risks to identity databases.

The scenario has several phases:

- Phase 1: Internet access and insiders.
    - The player must prevent attackers from modifying an identity database the must be accessible via the Internet. Potential solutions include use of network filters or VPNs. The attack motive is moderate, and thus filters and good policies (remote authentication and passwords) are sufficient.
    - One of the characters is bribed to maliciously modify the identity database, resulting in the issuance of bogus ID cards. The player must purchase at least "low" background checks for the staff of the Federal Identity Facility. This causes the offending character to be replaced by a more trustworthy character.
- Phase 2: Access control
    - A contractor requires remote read-only access to the identity database. The contractor also has Internet connections and the contractor does

not secure these Internet connections. As a result, attackers can use the contractor's system to access the identity database. The best the player can do is to set ACLs on the identity database to limit the contractor to read-only access.

- Phase 3:
    - Player is enticed to replace a physical guard with a smart card controlled smart lock. The guard had been protecting a very high value asset. If the player makes this choice, then the attacker's motive to compromise the identity database rises to the motive of the asset protected by the smart lock.