The Principle of Confidentiality

Director of National Intelligence Privacy and Civil Liberties Office

1. With respect to "confidentiality," the insider threat program must consider all the usual Fair Information Practices (e.g., notice to the workforce) and the necessary privacy and security safeguards, including:

    - Role-based access to the data, and
    - Oversight of the program personnel and system administrators (watch the watchers)

2. Limitations on the sharing of derogatory information should be considered when following up on reports. The derogatory information should be shared only with an agency component in a position to confirm or deny an allegation. The information should be reviewed to ensure it is accurate before it may be acted on. The insider threat program should also ensure that any inaccuracies it has found are remedied and corrections passed along to recipients of the erroneous data.

3. It is important to prevent any negligent impugning of an individual's reputation or professional status. If an error results in harm to an individual's prospects for continued employment or future employment, redress must be afforded.

4. Reported information may only be used for the purpose reported; it may not have any secondary uses unrelated to the insider threat activity. Finally, it may be necessary to establish or amend an agency's System of Records Notice (SORN) to ensure compliance with the Privacy Act.

5. It is vital that all employees know what to expect regarding confidentiality and process. Employees and other covered persons should be provided the address/link of the applicable Privacy Impact Assessment(s), System of Record Notice(s), and Departmental directive(s), instruction(s), and SOP(s).

6. Login banners must comply with your organizations requirements and associated policy. The Office of the Chief Information Officer (OCIO) should communicate to all persons with login credentials the content of the login banner.