IT Specialist (Security) - 2210

Development of IT Security Policies and Procedures

- Comprehensively analyze HHS, NIH, and other Government/industry/academe policies and procedures.
- Write [IC] specific policies to implement appropriate policies and procedures. Documents are clearly written, well organized, and encompass all situations, including actions to be taken in the event of an IT security violation.

Risk and Vulnerability Analyses

- Perform comprehensive and in-depth risk and vulnerability analyses on [insert number or percentage] of [IC]'s systems.
- Remediate problems found within established timeframes and due dates.
- Proactively modify policies and/or procedures to avoid repetition of problems found by analyses.

IT Security Training

- Coordinate or personally conduct annual security training while properly using audio visual equipment, showing knowledge of the subject, communicating courteously and clearly, and responding to all customer questions.
- Courteously notify users of the requirement for IT security training within established due dates.
- Accurately track IC's percentage of IT security training completion.
- On a proactive basis, disable accounts of users that have not completed the required training.

IT Security – As Part of System Design

- Consistently provide prompt, accurate, and comprehensive information to design groups to ensure IT security is designed into IT systems from the beginning.
- Proactively review system designs from an IT security standpoint and propose well-documented changes as required.

Effectively React to IT Security Events

- Within agreed-upon due dates, facilitate the gathering, analysis, and preservation of evidence used in the prosecution of computer crimes in an organized and accurate manner.
- Assess security events to appropriately determine impact and implement corrective actions. Documentation of assessments is consistently thorough, accurate, and timely.
- Provide information to appropriate law enforcement personnel as necessary to deal with IT security violations. Information must be thorough, accurate, and timely.