Information Security Specialist - Office of the Inspector General (ID: 23544)

The Information Security Specialist performs technical automation and compliance analysis related to information technology security issues. Conducts, and sometimes leads, special studies and projects relating to information security-related legislation and implementing regulations (such as cybersecurity or computer forensic analysis), and Board information security practices and policies. This position is responsible for Federal Information Security Modernization Act (FISMA) compliance —as implemented at the Board— within the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) and the Consumer Financial Protection Bureau (CFPB). The IS specialist develops and implements security policies and procedures to ensure the confidentiality, integrity, and availability of OIG applications and systems. Supports the OIG with information security matters, and general documentation for information security and compliance. This position requires knowledge of information security standards and practices, relevant legislative requirements, and overall information technology expertise.

KNOWLEDGE/SKILL REQUIREMENTS

At the FR-26 grade, bachelor's degree from an accredited college or university in information technology, computer science or related field, or equivalent experience, plus at least 5 years of progressive experience in information security or compliance. Must have demonstrated knowledge of and competence in the application of security to advanced IT systems. Strong technical writing experience is required, as well as demonstrated ability to research and formulate recommendations on complex IT and compliance issues. Requires excellent analytical ability in oral and written communications. Requires a broad knowledge of general IT security theory and practices. Experience performing security reviews and control testing required. Knowledge of information security compliance and implementation of security architectures and related standards. Possesses knowledge of the laws and regulations governing all aspects of IT security as it relates to the government. Knowledge and experience with FISMA requirements, NIST security guidance, and OMB security mandates required.

Requires a strong customer service philosophy, flexibility, commitment to teamwork, and good research skills. Must have demonstrated experience in coordinating work assignments and the ability to work on multiple projects simultaneously while meeting critical deadlines. Able to adjust to changing priorities & customer needs desirable. Ability to brief management and recommend specific actions. Must be detail-oriented and committed to excellent customer service. Demonstrates sensitivity to individuals, organizational relationships, and project management requirements. High degree of proficiency in oral and written communication skills. Excellent interpersonal skills and ability to work well in a team environment. Ability to obtain a Top-Secret clearance and is subject to the Board's drug testing program.

In addition to the FR-26 Knowledge/Skill Requirements, at the FR-27 grade, must have at least 6 years of progressive experience in information security or compliance. knowledge and experience with project management methodology, and a proven track record of delivering complex technical projects according to schedule.

About Us – OIG

REMARKS

- Knowledge of federal IT initiatives, including zero trust architecture, cloud computing, supply chain risk management, and SDLC is preferred.
- Past performance evaluations may be requested

- The OIG's interim telework policy requires employees to be physically present in the office a minimum of 4 days per month. Employees may be expected to be physically present in the office more than 4 days per month, as required by business needs. The OIG will revisit its interim policy towards the end of 2023 to determine whether any changes will be made.