Office of the Inspector General (OIG), Technology Services (TS)
Supervisory Information Technology Specialist, GS-2210-15
Detail/Temporary Promotion Opportunity

The U.S. Department of Education, Office of Inspector General (ED OIG) is looking for a highly motivated Supervisory Information Technology Specialist (GS-15) to serve on a **reimbursable** 120-day detail, beginning on/about October 19, 2025, which may be extended if all parties are in agreement. The selectee will serve as the Chief Technology Officer in the Technology Services (TS) component and will report directly to the Acting Assistant Inspector General for Technology Services.

ED OIG is a dynamic, high-performing oversight organization with a diverse, inclusive, engaged and skilled workforce. We are a mid-sized OIG, and our collaborative staff work closely together to ensure the integrity, transparency, and efficiency of Federal education programs and operations. This is a growth opportunity that will prepare you for entry into the Senior Executive Service by tackling the leading challenges of a technology services group responsible for cybersecurity, customer support, and the management of a multi-million-dollar budget that supports the information technology needs of an oversight body that affects every student in America.

For ED OIG employees: This opportunity may be filled as a temporary promotion and or detail assignment at their current grade and salary.

For OIG employees outside of ED OIG: This opportunity will only be filled as a reimbursable detail assignment at the candidates' current grade and salary through an Interagency Agreement (IAA).

Duty Location:

The position can be performed from any federal office in the United States in compliance with the Presidential Memorandum *Return to In-Person Work. This position is not eligible for telework or remote work.*

Duties:

Supervises and directs the work of Information Technology specialists in the day-to-day operation, maintenance, and security of the OIG IT infrastructure. Evaluates subordinates' performance; approves leave; recommends promotions, reassignments, and disciplinary measures. Keeps employees informed of OIG goals and objectives.

Develops, implements, oversees, and monitors a program of assessment and authorization for OIG systems, data, and infrastructure to ensure that all systems have a valid Authority to Operate (ATO).

Ensures the proper integration of Information Technology programs and services; and develops solutions to integration/interoperability issues. Designs, develops, and manages systems that meet current and emerging business requirements and apply and extend or optimize the existing architecture.

Establishes and executes configuration management process to properly develop, manage, maintain, and document the current and future OIG systems.

Lead, maintain and coordinate activities (such as creating PowerBI Dashboard, Workflows, Network/IT Infrastructure Upgrades) to support an organization's office automation efforts.

Independently serves as a senior IT expert and consultant to OIG management officials and staff at Headquarters and Regional Offices. Ensures development of a secure technical architecture and plan for integrating security into programs and the agency's IT structure meeting OIG operational requirements.

Ensure compliance with Federal Information Security Modernization Act (FISMA) of 2014, FedRAMP, National Institute of Standards and Technology, and Departmental directives and guidelines.

Independently spearheads and leads ad hoc teams to ensure that all technical, physical, security, and procedural requirements are fulfilled for the OIG. Reviews current legislation, statutes, regulations, and other security resource information and ensures that the OIG systems' security posture is aligned with current practices. Ensures that individuals within the OIG are trained on current and emerging technologies for effective/efficient use of technologies. Assists in conducting IT system operations and security reviews, developing, and implementing policies and providing educational lectures and briefings.

Develops and implements Information system operation program that assesses and addresses the effective and proper use of systems and risks and magnitude of the harm resulting from the loss, misuse, or unauthorized access of information. Ensures that information systems used by the OIG operate in a secure manner and provides appropriate confidentiality, integrity, and availability using cost-effective management, administrative, operational, and technical controls.

Participates in studies and analyses and maintains knowledge of threats to information systems and data; establishes information assurance objectives, operational processes, and appropriate counter-measures to defend OIG systems and data against identified threats; and develops, implements, oversees, and monitors IT security strategies, plans, policies, agreements, standards, practices, and security management programs to ensure OIG system and data compliance with statutes like the Federal Information Security Management Act and with Office of Management and Budget (OMB)/Department/OIG regulations and guidelines.

Qualifications:

Minimum Qualification Requirements:

You may meet the minimum requirements for the GS-15 if you possess:

One year of specialized experience that equipped the applicant with the particular knowledge, skills, and abilities to perform successfully the duties of the position, and that is typically in or related to the work of the position to be filled. To be creditable, specialized experience must have been equivalent to the GS-14 level in the Federal government.

Specialized Experience for the GS-15:

One year of experience equivalent to the GS-14 performing all three (3) of the following duties or work assignments:

1. Expert experience in ensuring that information systems operate in a secure manner and ensuring appropriate confidentiality, integrity and availability through the cost- effective management, administrative, operational, and technical controls.
2. Expert experience in applying new developments to previously unsolvable security problems; making decisions or recommendations that significantly influence important information Assurance policies and programs.
3. Expert experience in applying project management principles, methods, and practices including developing plans and schedules, estimating resource requirements, defining milestones and deliverables, monitoring activities, and evaluating and reporting on accomplishments.

How to Apply:

Interested employees should obtain their supervisor's approval before requesting consideration for this opportunity. If interested in applying and you have obtained your supervisor's approval, please submit your resume via e-mail to Teresa.Dargan@ed.gov by ***September 5, 2025***.