DEPARTMENT OF THE TREASURY, DEPARTMENTAL OFFICES (HQ)

OFFICE OF THE CHIEF INFORMATION OFFICER, CYBERSECURITY

Background: Departmental Offices Local Area Network (DO LAN)

The DO LAN provides information management resources and support operations to the local Washington D.C. Treasury facilities, permits workstations to access network server resources and the Intranet, provides access to the Internet, and hosts Treasury applications. These resources include commercial office support and productivity applications, Word processing, spreadsheets, electronic mail, presentation graphics, network management and operations applications, and specialized applications unique to the Treasury mission. The DO LAN is also used to support, process, and store administrative, financial, investigative, personnel, and training information. It serves approximately 3,500 local users and approximately 2,400 remote users. The DO LAN includes application, file/print, data backups, communication, utility and management servers, network cabling, routers, switches, gateways, and other communications equipment required to support network connectivity

We are currently looking to fill permanent positions to work in the following areas:

Vulnerability Assessments

This position assists with the implementation of Office of the CIO Enterprise Risk Management Strategy. This individuals primary duties include: a) Enhance the current vulnerability scanning program to ensure full monthly scanning of every IT asset within the organization's environment; b) Deploy enterprise tools to facilitate full monthly scanning, as well as collection and consolidation of the results; c) Assist System Owners and Information System Security Officers (ISSOs) with prioritizing and remediating noted vulnerabilities, and report to upper management; and d) Evaluate organization processes and perform threat analysis.

Mobile Devices

This position will work on the deployment of a new Mobile Device Management system and the implementation and management of a Wireless Intrusion Protection System (WIPS). The deployment of the WIPS will involve working with contractors to design the system, determine sensor locations, review technical results, and support installation. Once installed, policies/rules for the WIPS will be determined based on the results of the scan data received from the sensors. In addition to the WIPS, ad hoc manual wireless scans will be performed to validate results from the WIPS. The tools used for the WIPS are AirTight sensors and management console. The tools used for the ad hoc scans will range from Kismet, Fluke AirCheck, Fluke Air Magnet, and other wireless tools. This position will also review configurations for mobile devices and conduct vulnerability tests.

Software Risk Assessment

As a Software Risk Assessor, your responsibilities would be to conduct assessments on existing and requested Treasury software. Risk assessments shall take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to the organization's operations, assets, or individuals based on the operation of the information system. Risk assessments shall also take into account any risk posed to operations, assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational

information systems, outsourcing entities, foreign intelligence services, malicious or negligent insiders, malicious outsiders and any party with a vested interest in the success or failure of the system or the reputation of the Treasury Department). If risks are identified that are unacceptable to the Authorizing Official, the risk assessment shall identify additional control needs, provide cost-effective recommendations for mitigation, and determine resources to implement corrective action.