



SecureOffice® Trusted Releaser™

BENEFITS

- Enables secure, automated one-way bulk data transfer to lower-classified domain(s)
- Permits transfer of any data type
- Uses known legacy applications for review during transfer process
- Uses DoD X.509 digital certificate to implement former draft Inter-Domain Transfer Policy
- Processes CAPCO metatag markings in HTML and ICML documents
- Runs automatic security scans on all content based upon site security policy
- Flexible dirty word list
- Performs link checking on Web content targeted for lower levels

SECURE HIGH-TO-LOW TRANSFER OF DATA ACROSS NETWORKS

SecureOffice® Trusted Releaser™ is a high-to-low guard that provides secure, one-way transfer of bulk data from one security domain to one or more lower-classified domain(s). It facilitates the dissemination of sanitized information across security boundaries, making critical data available to the war fighter immediately.

Transfer of Multiple Data Types, No Proprietary Review Software

Trusted Releaser can transfer large quantities of practically any type of data (Web content, maps, imagery, Microsoft® documents, etc.) from any operating system (UNIX® or Microsoft®) or in any format, fixed or variable. Unlike other guards, the system does not require proprietary software to view and process each data type. The user utilizes standard applications to create, manipulate and view data intended for dissemination.

Two-Person Review Automated Process

Trusted Releaser implements the Defense Intelligence Agency's (DIA's) Reliable Human Review process for all data targeted for dissemination to a lower security level. The first person of this two-person review process is the Producer who is responsible for initial selection of files for relabeling and initial security review. The second reviewer, the Releaser, is a designated Release Authority (or Foreign Disclosure Officer) responsible for verifying the validity of the Producer's release determination.

A simple Java-based application, supported on both Windows® and UNIX® platforms, is used by both reviewers. The reviewer selects a bundle of files and destination security level(s), performs a

link check, dirty word search and visual content verification and then appends a digital certificate to the file bundle. The processed file bundle is submitted to the Trusted Releaser for final validation and processing. Trusted Releaser verifies that both a Producer and an authorized Releaser have digitally signed the file bundle. It then virus scans the bundle and moves the bundle into a designated directory and/or server on the destination security level network(s).

Multiple Features for Enhanced Security

Trusted Releaser offers various security features that help ensure a reliable and safe means of transferring data. It automates the Intelligence Community's former draft, two-person, human review Inter-Domain Transfer Policy, and it employs Department of Defense (DoD) and Intelligence Community PKI/X.509 digital certificates for the signing of data to be transferred in keeping with DCID 6/3 requirements for Strong Authentication. It includes IP packet filtering, as well as role-based administration, mandatory access controls (MAC), use of least privilege and removal of the super-user root account. As each file is transferred across levels, the file is virus scanned for Microsoft®-type PC viruses, and all files are dirty word scanned against an administratively defined library of terms.

Top-Level Security Approval

Trusted Releaser was developed to support the Intelink Management Office's (IMO) transfer of INTELINK Web Data from TS/SCI to SECRET. Trusted Releaser is a plug-in component of the National Security Agency (NSA)-assessed and DIA-approved SecureOffice® Trusted Gateway™. Trusted Releaser is the dissemination component of DIA's Multi-Domain Dissemination System (MDDS).