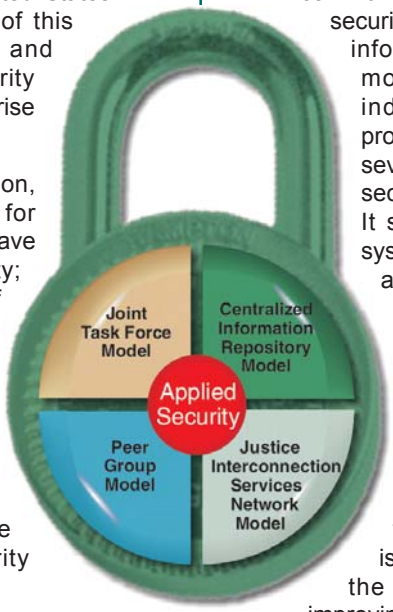
Executive Summary

Applying Security Practices

to Justice Information Sharing

Applying Security Practices to Justice Information Sharing was developed through a collaborative effort of the Security Working Group of the Global Justice Information Sharing Initiative (Global), Office of Justice Programs (OJP), United States Department of Justice (DOJ). The purpose of this document is to educate justice executives and managers in good, basic, foundational security practices that they can deploy within their enterprise and between multiple enterprises.

This document contains background information, overviews of best practices, and guidelines for secure information sharing. Fifteen domains have been identified—governance; physical security; personnel security screening; separation of duties; identification and authentication; authorization and access control; data integrity; data classification; change management; privacy and confidentiality; firewalls, virtual private networks (VPNs), and other network safeguards; intrusion detection systems; critical incident response; security auditing; and disaster recovery and business continuity—that span the important elements of an information security architecture.



This document is not intended to suggest a standard security approach, nor is it intended to provide an in-depth security solution for any particular system. It is also not intended to provide detailed technical reference for system administrators.

Many of these suggested practices are low-cost in that they require users to be educated about security practices and suggest awareness and evaluation of the security threat. Other practices require capital investment and continued maintenance to ensure their effectiveness. However, doing nothing can also have unacceptable associated costs.

The appropriate application of security practices is highly dependent upon the specifics of the information systems to be protected. Characteristics such as connectivity to public networks, the scope and composition of the user community, the sensitivity of the information, and the level of acceptable risk should all have strong influences on the security approach used. This document provides further guidance to justice information system managers and owners by defining general models for justice information sharing, recommending security guidelines, and citing usage examples. It includes four justice information sharing models that are frequently encountered in justice applications:

- The Joint Task Force Model
- The Centralized Information Repository Model
- The Peer Group Model
- The Justice Interconnection Services Network Model

www.it.ojp.gov

These four models are simplified representations of the organizational relationships, computer systems, and the flow of information encountered in the justice and public safety communities. They serve as illustrations of "best-of-breed" security practices. In application, most "real life" justice information systems are a combination of these models, although they are described here individually. Justice information systems professionals faced with an enterprise that combines several of the models will need to identify common security services that can apply to all of their systems. It should be noted that some justice information systems professionals may unpredictably encounter a fifth model: the disorganized, fragmented, run-by-another-part-of-the-city model.

The long-term goal is to enable an environment of electronic trust among law enforcement and justice organizations. Electronic trust will be engendered if each organization can be assured that all parties with access to shared information will follow certain minimum practices to safeguard that information. An environment of electronic trust is a minimum requirement for us to begin to fulfill the national priority of sharing information and improving the safety of the country. It must be recognized that justice information technology systems are a vital part of the nation's critical infrastructure, and as such, information technology infrastructure requires comprehensive security architecture. Protecting this critical resource is not just a matter of operational good sense; it is increasingly a matter of national security and public safety.

Applying Security Practices to Justice Information Sharing

Detection and Recovery
- Intrusion Detection System
- Critical Incident Response
- Security Auditing
- Disaster Recovery and Business Continuity

Prevention
- Data Integrity
- Data Classification
- Change Management
- Firewalls, VPNs, and Other Network Safeguards
- Identification and Authentification
- Authorization and Access Control
- Privacy and Confidentiality

Support
- Governance
- Physical Security
- Personnel Security Screening
- Separation of Duties