Federal Information Security Management Act

The **Federal Information Security Management Act** (**FISMA**) is a United States federal law as Title III of the **E-Government Act**. The act recognizes the importance of information security to the economic and national security interests of the United States. The act requires agencies to develop, document, and implement programs that provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by a contractor or other source. The E-Government Act is a United States statute. Its stated purpose is to improve the management and promotion of electronic services and processes by establishing a framework of measures for Internet-based information technology. With regard to compliance, there is no option; ALL government agencies MUST COMPLY with the mandates of both acts.

FISMA legislation was enacted in 2002, came into force in April of 2003 and has brought attention within the federal government to cyber security and explicitly emphasized a "risk-based policy for cost-effective security."

According to FISMA, the term *information security* means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality and availability.

Compliance framework defined by FISMA and supporting standards

FISMA must be followed by all government agencies for all information systems used or operated in the executive or legislative branches, or by a contractor or other organization on behalf of a federal agency. The compliance framework defines of several key areas of concern. The primary areas as they relate to data collection are as follows:

- **Inventory of information systems**
  FISMA requires that agencies have in place an information systems inventory. There is not a direct mapping of computers to information system; rather, an information system may be a collection of individual computers put to a common purpose and managed by the same system owner.
- **Security controls**
  Organizations must meet the minimum security requirements. Agencies have flexibility in applying the baseline security controls. This allows agencies to adjust the security controls to more closely fit their mission requirements and operational environments.
- **Risk assessment**
  A foundational level of security for all federal information and information systems is required. The agency determines and validates security controls to protect agency operations, assets, and individuals. Risk is determined by calculating the likelihood and impact that any given vulnerability could be exploited.
- **Continuous monitoring**
  Systems are required to monitor a selected set of security controls. Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. The organization establishes the schedule for control monitoring.

Print Tracker is Federal Information Security Management Act compliant because the software can be installed on any managed computer or system, does not increase risk vulnerability or allow changes to systems or security controls, and the information it gathers can be used to maintain cost objectives for any government agency.

Print Tracker is a software tool that gathers meters and status information from imaging devices like copiers and printers. It contacts network devices using their IP addresses and requests device information via the Simple Network Management Protocol (SNMP). Communication is fulfilled via port 161. If SNMP provided information is incomplete, Print Tracker may request data from the device's embedded web server over port 80. Collected information includes the device's network name, MAC address, model, serial number, total page counter, color page counter, prints, copies, faxes, scans, location, and status. Print Tracker CANNOT gather printed content or interpret user intent. If desired, IP addresses of devices may be blocked from reporting.

Imaging device data that Print Tracker captures is encrypted and sent to a secure web server using the HTTPS protocol over port 443. The secure web server addresses used include https://secure.tc101.com and https://secure.nexation4.com. All data transfer is encrypted and initiated on site at the deployment location. There is no remote access option with Print Tracker and Print Tracker CANNOT receive incoming transmission.

The information offered above was obtained from the following sources:
http://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002
http://en.wikipedia.org/wiki/E-Government_Act_of_2002