



# Biotech Security: FDA 21 CFR Part 11

An informational presentation to the TOG Security Forum on life sciences security regulations and requirements



Mike Jerbic

Trusted Systems Consulting Group

*Mjerbic@trustedsystemsconsulting.com*

408.257.1648

# Agenda

- Security drivers and threats in the drug development industry
- FDA regulatory interests
- 21 CFR Part 11 Security and Electronic Signature Standards
- Other security concerns in the biotech industry
- Open issues and discussion



# Drug Development Business Environment

- Heavily regulated industry (US Food and Drug Administration)
- Drugs routinely take 13 years and \$500M investment to develop
- 17 year patent life leaves only about 4 years to recoup investment and make profit
- Drug researchers and developers often have financial incentives to produce/deliver
- Objective: FDA Approval in minimum time

# FDA Mission

*(source [www.fda.gov](http://www.fda.gov))*

The FDA Modernization Act of 1997 (PL 105-115) affirmed FDA's public health protection role and defined the Agency's mission:

- To promote the public health by promptly and efficiently reviewing clinical research and taking appropriate action on the marketing of regulated products in a timely manner;
- With respect to such products, protect the public health by ensuring that foods are safe, wholesome, sanitary, and properly labeled; human and veterinary drugs are safe and effective; there is reasonable assurance of the safety and effectiveness of devices intended for human use; cosmetics are safe and properly labeled, and; public health and safety are protected from electronic product radiation;
- Participate through appropriate processes with representatives of other countries to reduce the burden of regulation, harmonize regulatory requirements, and achieve appropriate reciprocal arrangements; and,
- As determined to be appropriate by the Secretary, carry out paragraphs (1) through (3) in consultation with experts in science, medicine, and public health, and in cooperation with consumers, users, manufacturers, importers, packers, distributors and retailers of regulated products.

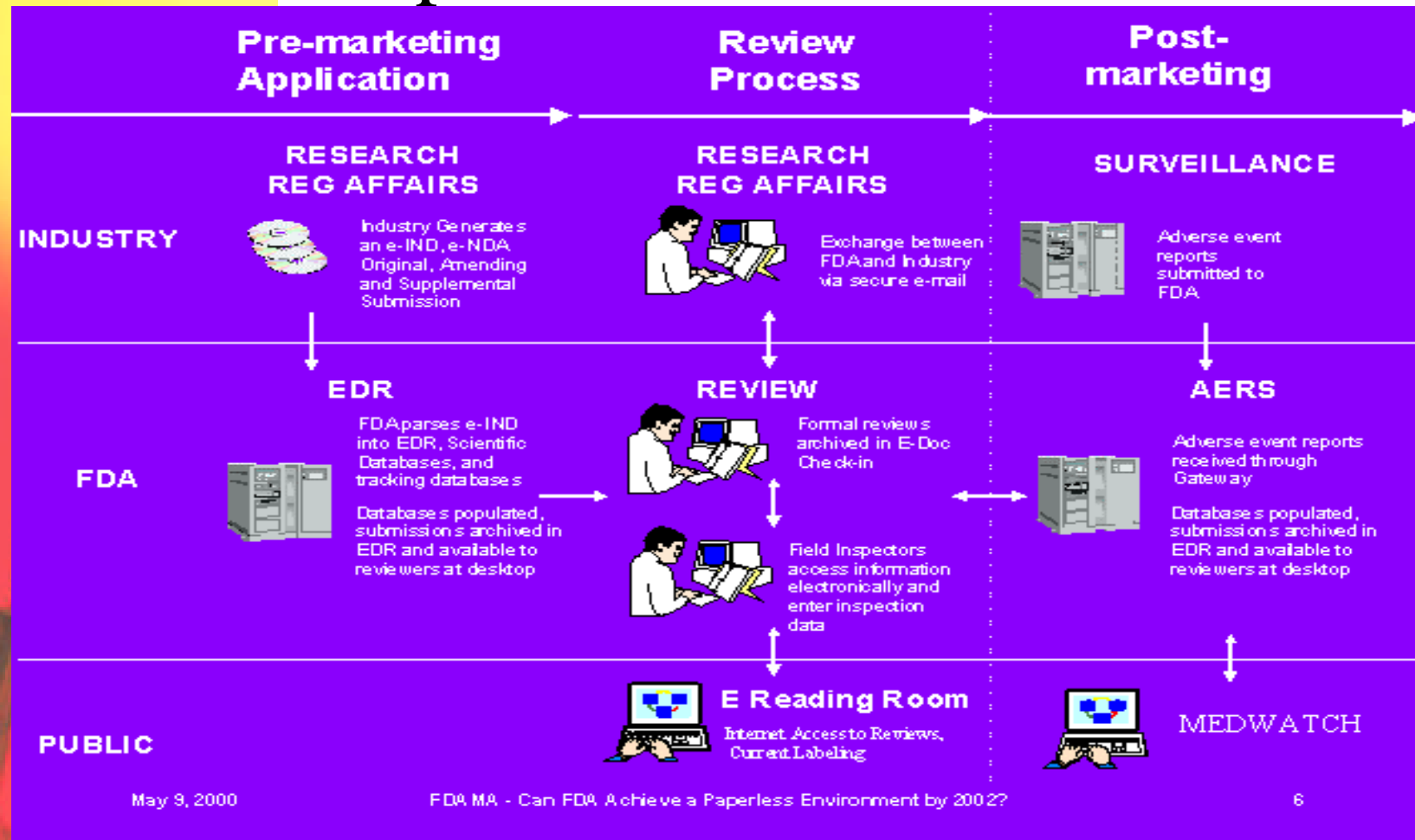


# Products the FDA Regulates

*(source [www.fda.gov](http://www.fda.gov))*

- Food
  - Foodborne illness, nutrition, dietary supplements
- Drugs
  - Prescription, Over-the-counter, generic
- Medical Devices
  - Pacemakers, contact lenses, hearing aids
- Biologics
  - Vaccines, blood products
- Animal feed and drugs
  - Livestock, pets
- Cosmetics
  - Safety, labelling
- Radiation-emitting products
  - Cell phones, lasers, microwaves

# Situation Assessment: FDA and a Paperless Environment



(source: <http://www.fda.gov/cder/present/phrma5-2000/lillie/sld001.htm>)



# Security and Electronic Signature Standards – FDA Interests

- Consider electronic records and signatures to be the full equivalent to paper records and traditional handwritten signatures
- Permit the widest possible use of electronic technology, compatible with FDA's responsibility to promote and protect public health
- Use of electronic records and their submission is voluntary (but...)
- Set example for other Federal Government agencies in accepting electronic records
  - Government Paperwork Elimination Act (GPEA) of 1998, requires that Federal agencies enable electronic reporting and record-keeping by 2003
  - EPA Cross-Media Electronic Reporting and Record-keeping Rule (CROMERR)

# Major Electronic Record and Signature Threats the FDA Worries About

- Fraud
- Unreliable, untrustworthy information submittals:
  - Information falsification
  - undetectable changes to information
  - “Selective” information used in studies
- Automated data generation and analysis tool correctness and reliability
- FDA falling behind in its analytical capability, putting the agency at a disadvantage compared to regulated industry



# Electronic Records: Expected Benefits

*for industry and regulators*

- Trustworthiness of electronic records equals that of paper records
- Increased speed of information exchange
- Reduced cost of information storage
- Reduced vulnerability to human error
- Improved regulatory effectiveness from data integration / trending
- Improved products
- Streamlined manufacturing
- Improved process controls
- Reduced vulnerability of electronic signatures to fraud and abuse

# FDA's Answer: 21 CFR Part 11

- Subpart A General Provisions
  - 11.1 Scope
  - 11.2 Implementation
  - 11.3 Definitions
- Subpart B Electronic Records
  - 11.10 Controls for closed systems
  - 11.30 Controls for open systems
  - 11.50 Signature manifestations
  - 11.70 Signature/record linking
- Subpart C Electronic Signatures
  - 11.100 General requirements
  - 11.200 Electronic signature components and controls
  - 11.300 Controls for identification codes/ passwords

# Scope and Applicability

- Applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations.
- Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.
- Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials and other general signings as required by agency regulations.
- Rule finalized March 20, 1997. Effective August 20, 1997.
- No “grandfathering” provisions for old, non-compliant equipment.
- Does not apply to paper documents transmitted electronically.

# Definitions

- **Electronic Record**
  - Any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system
- **Closed System**
  - An environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system
- **Open System**
  - An environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system
- **Digital Signature**
  - An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identify of the signer and the integrity of the data can be verified.
- **Electronic Signature**
  - A computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

# Controls for Closed Systems (1)

- Objectives
  - Ensure authenticity, integrity, and when appropriate confidentiality of electronic records and to ensure that the signer cannot readily repudiate signed records as not genuine
- Includes (21 CFR 11.10)
  - System validation to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records
  - Ability to generate accurate and complete copies of records in human readable and electronic form
  - Records protection to enable accurate and ready retrieval throughout the retention period
  - Limiting system access to authorized individuals

## Controls for Closed Systems (2)

- Includes (cont'd)
  - Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.
    - “provide a trail of who did what, wrote what, and when.”
  - Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.
  - Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

# Controls for Closed Systems (3)

- Includes (cont'd)
  - Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.
  - Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.
  - The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.
  - Use of appropriate controls over systems documentation including:
    - Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.
    - Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.



# Controls for Open Systems

- Objectives
  - Same as for closed systems
- Includes (21 CFR 11.30)
  - Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.



# Signature Manifestations and Record Linking

- Signed records must include
  - Printed name of the signer
  - Date and time when the signature was executed
  - Meaning (such as review, approval, responsibility, or authorship) associated with the signature
- Above items are also considered electronic records subject to the 21 CFR 11 controls and shall be included as part of any human readable form of the electronic record (such as electronic display or printout)
- Signature / Record Linking
  - Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

# Electronic Signatures

- General Properties

- Unique to one individual. Shall not be reused by or reassigned to anyone else (e.g user ID code and password)
- Organization must verify an individual's identity before assigning an electronic signature to him/her
- (Paper, handwritten) certification to FDA that use of electronic signature is intended to be legally equivalent to handwritten signature, such as:

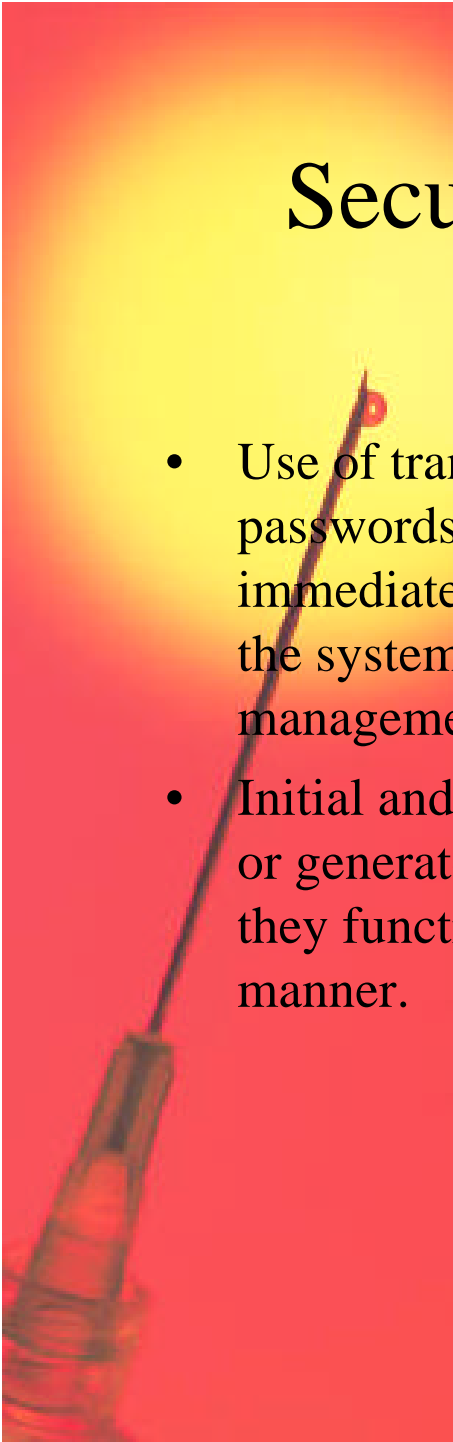
“Pursuant to Section 11.100 of Title 21 of the Code of Federal Regulations, this is to certify that [name of organization] intends that all electronic signatures executed by our employees, agents, or representatives, located anywhere in the world, are the legally binding equivalent of traditional handwritten signatures.”

# Electronic Signatures

- Components and Controls
  - Electronic signatures that are not based upon biometrics shall:
    - Employ at least two distinct identification components such as an identification code and password.
    - Be used only by their genuine owners; and
    - Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.
  - Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

# Security Controls for Identification Codes/Passwords

- Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.
- Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).
- Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

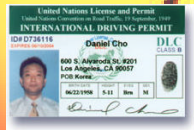


# Security Controls for Identification Codes/Passwords

- Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.
- Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

# Regulated Electronic Records

Creation • Modification • Maintenance • Archival • Retrieval • Transmittal



- Identity Verification
- Credential issuance
- Access rights, privileges
- Agreement to use of signatures, understanding of legal equivalence

Configuration Data  
e.g. device settings



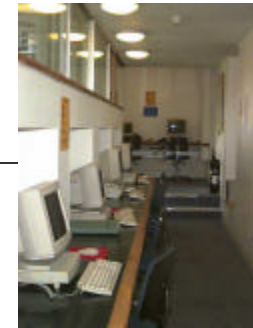
Data Generation  
e.g. output data

Analysis Tools  
e.g. spreadsheets, database reports, graphic display



Reports  
Reduced Data  
Relevant email  
FDA e-filings

Configuration Data  
e.g. cfg files, access controls



IT Infrastructure  
Document Mgmt  
Database, storage  
E-Communications  
Hardcopy I/O  
Infrastructure Services

Validation • Authorization • Protection • Audit • System Checks • Device Checks  
Training • Policies for Accountability • Documentation and Change Controls

# Personal Conclusions

- The FDA is suspicious of information submitted to it and therefore has high standards for data authenticity/integrity and submitter accountability
- Software is not assumed to work and must be validated for use in . This is / will be a big issue. Where to draw the line?
  - “The agency disagrees with the comment’s claim that all commercial software has been validated. The agency believes that commercial availability is no guarantee that software has undergone “thorough validation” and is unaware of any regulatory entity that has jurisdiction over general purpose software producers. The agency notes that, in general, commercial software packages are accompanied not by statements of suitability or compliance with established standards, but rather by disclaimers as to their fitness for use. The agency is aware of the complex and sometimes controversial issues in validating commercial software. However, the need to validate such software is not diminished by the fact that it was not written by those who will use the software.”

## Personal Conclusions (2)

- People don't know what to audit. How far in the "system" do you go to achieve who did what when?
- Non compliant lab equipment is and will be a problem as paper output becomes obsolete
- Other Federal agencies will follow the FDA's lead and use 21 CFR 11 as a model
  - EPA CROMERR
- System validation, especially of integrated software from multiple vendors, remains a substantial challenge to manage effectively



# What's Next

- Compliance costing industry much more than anticipated
- Movement to a “risk-based” approach
- Change of leadership within the FDA – different perspectives?
- A new release of the rules and regulations sometime in the future

# Other Biotech Security Concerns

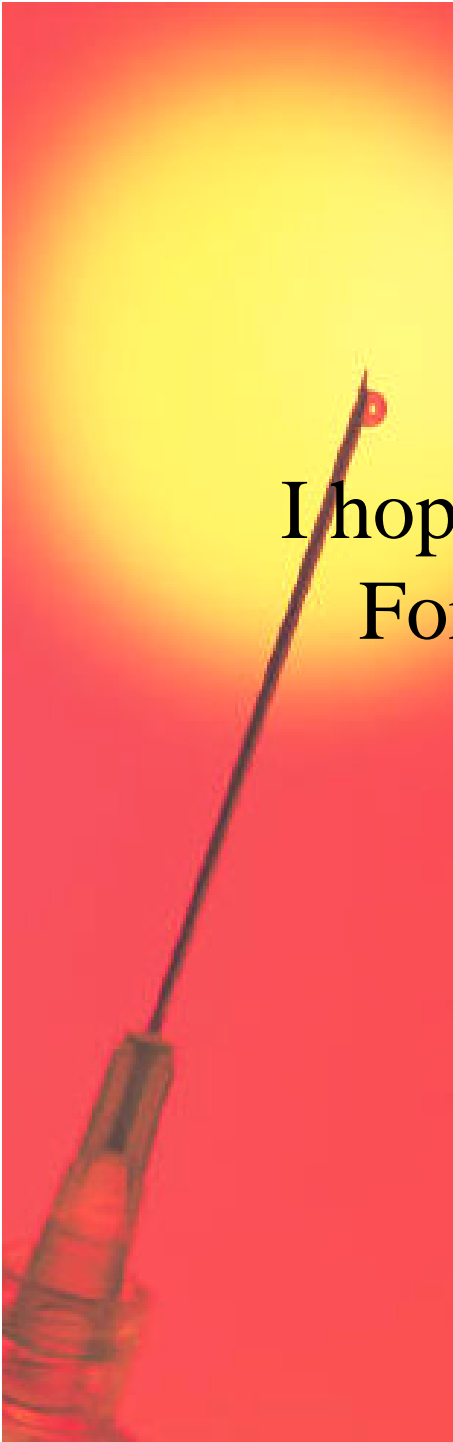
- Key “ordinary issues” are hard for this community to solve
  - Secure email
  - Single signon, “integrating Kerberos with PKI”
  - TOG Security Forum can help?
- Life sciences community doesn’t know what needs to be secured
  - Run by researchers, not production practitioners
- National Security, Bioterrorism, Scientific Openness
  - **The National Academies and CSIS to Host Jan. 9 Meeting on National Security and Scientific Openness**

WASHINGTON -- The National Academies and the Center for Strategic and International Studies will co-host a public meeting on Jan. 9 to bring together scientists and policy-makers to discuss whether current publication policies and practices in the life sciences could lead to the inadvertent disclosure of "sensitive" information to those who might misuse it. The goal of this meeting is to start a dialogue between the life sciences and national security communities that might eventually lead to the development of a common set of publication policies for journals in the life sciences.

- Genome, Genetic data security and privacy
  - A Security System for Personal Genome Information at DNA level
- Genetic research intellectual property protection
  - “use the model without disclosing the model”

# Other Biotech Security Concerns

- “Endpoint security”
  - Anonymous access of the genomic and other information and services
- HIPAA Security Regulations
  - Privacy regulated. Security “sufficient to ensure privacy”
  - Security regulations could come in future (45 CFR Part 142 Security and Electronic Signature Standards; Proposed Rule put forward August, 12, 1998, no finalization)



I hope you found this presentation valuable.  
For further information, please contact:

Mike Jerbic

Trusted Systems Consulting Group

[Mjerbic@trustedsystemsconsulting.com](mailto:Mjerbic@trustedsystemsconsulting.com)

408.257.1648

# About Mike Jerbic



Mike Jerbic, the firm's principal consultant is an information security professional with 10 years of experience in engineering, management, and development of Hewlett-Packard enterprise security products. He directed the utility services program for HP's disaster recovery product "Data Protector," and the security, systems management, repository, and networking program for "E-Speak," a distributed a Web Services framework. Prior to that he managed HP's UNIX operating system's kernel and commands security project for seven years where he led the release of Common Data Security Architecture, Pluggable Authentication, Trusted NIS+, all the while improving quality and eliminating legacy UNIX vulnerabilities. Before becoming a manager, he served as developer, and later architect, of PC storage systems at HP. His combination of development and management experiences make him a pragmatic strategist.

Active in his profession, Mike contributes his time and expertise to a number of professional organizations including:

- The Open Group Security Forum
- Interoperable Informatics Infrastructure Consortium
- The American Bar Association's Information Security Committee
- San Francisco Bay Infragard
- The Silicon Valley Chapter of the Project Management Institute



# About Trusted Systems Consulting Group

- Who we are

Trusted Systems Consulting Group consists of a network of experienced enterprise systems information security professionals with engineering, management, and legal experience in the high tech industry. We have deep experience in the development and deployment of enterprise platform, middleware, application, and business continuity security products, having worked with major accounts in many industries solving digital signature, information integrity, and assurance problems. We focus on solving business problems, taking a broad view of the client's security needs and current system to identify pragmatic, cost-effective solutions. This approach minimizes business disruption, solves the client's security problems for the long term, and minimizes overall cost of ownership.

- Our Services

- Policy assessment and development
- IT project development services including implementation, and project management
- Product development services including engineering, product management, project management, and program management
- Systems assessment and validation
- Operations analysis and optimization
- Training and awareness building
- Regulatory Compliance consulting

- We want to work with you. To contact us:

- [Mjerbic@trustedsystemsconsulting.com](mailto:Mjerbic@trustedsystemsconsulting.com)
- 408.257.1648