

# e-Diagnostics System and Data Security

**Mike Sigman**

Director, Information Technology

International SEMATECH

mike.sigman@sematech.org, 512-356-7806

October 19, 2000

# System Security



- Semiconductor Manufacturers IT Security Council is a Council of International SEMATECH Member Companies formed to address IT Security issues prevalent in Semiconductor Manufacturing
- Council Developed e-Diagnostics Security Guidelines in cooperation with the full e-Diagnostics team

# e-Diagnostics Security Guidelines V1.1

## Purpose/Scope:

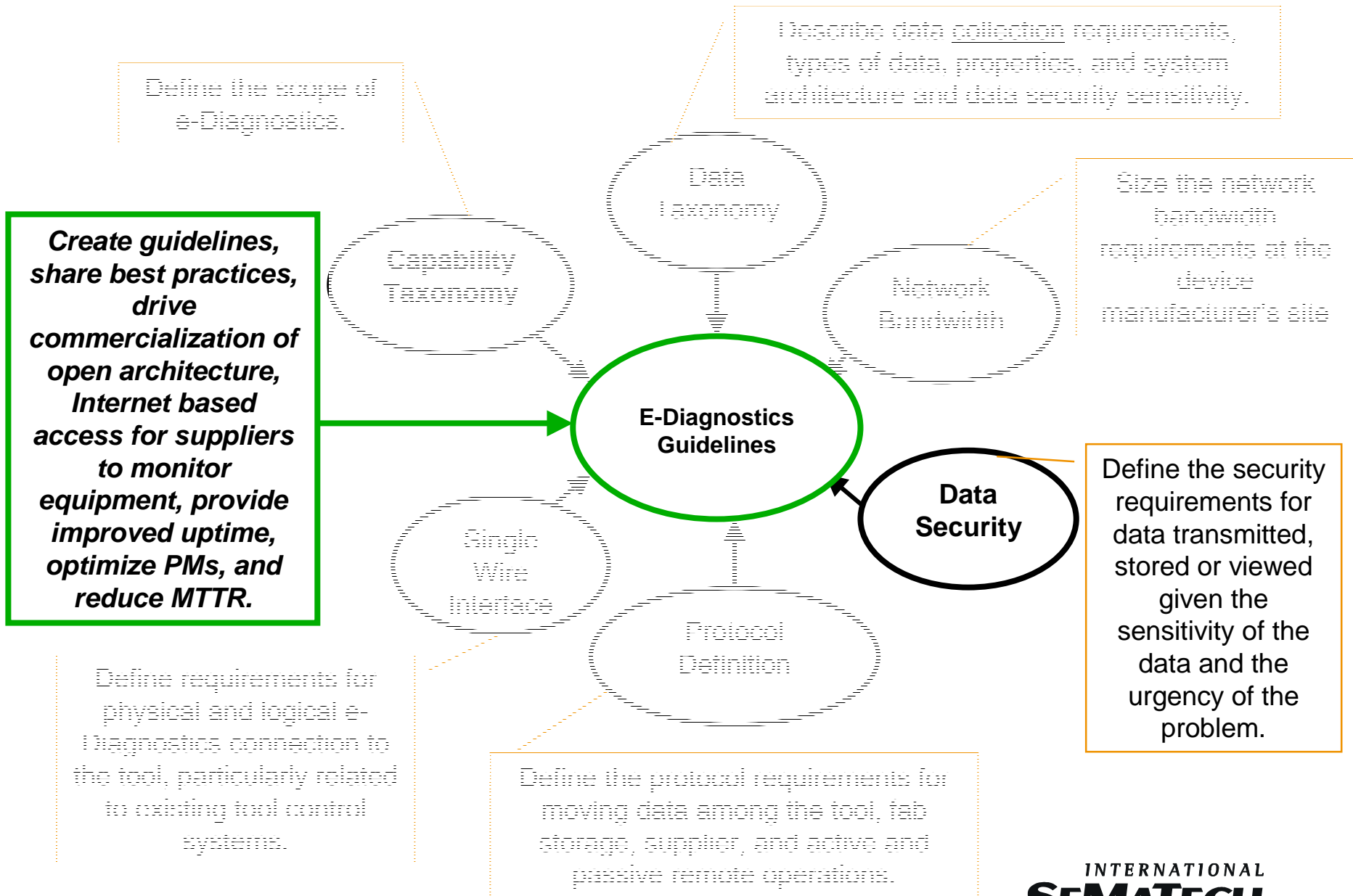
Define Information Technology security guidelines to support e-Diagnostics as defined in the International SEMATECH e-Diagnostic Guidelines. All guidelines apply to individual factory tools as well as any intermediate storage or concentration areas. Intellectual property protections, such as recipe content are addressed by the e-Diagnostics team and are beyond the scope of this document.

1. System, including security, must be based on non-proprietary networking and computer architecture.
2. System must meet or exceed standard Information Technology security practices, as defined in BS 7799 (Draft ISO 17799.)
3. Communication must take place over standard communication connections using TCP/IP protocols. Legacy serial connections may be used for low bandwidth tools.
4. All remote access must be from only known identifiable sources using techniques such as PKI digital certificates validated by an agreed certificate authority, handheld authenticators or biometric techniques.

# e-Diagnostics Security Guidelines V1.1 (cont.)

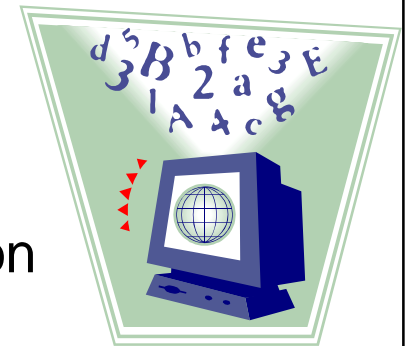
5. Data transmission and external storage must have the capability to be encrypted using standard publicly available secure methods in compliance with export control restrictions. All Internet and Extranet based remote access and storage must be secure and encrypted. Intranet based remote access and storage is at customer discretion.
6. Audit trails, including who, what and when must be maintained for all data transfers and any remotely initiated changes.
7. System must support detailed access control at the data item level for read, write, and remote control functions.
8. System must function as part of a single network connection to the tool. It must also be capable of being supported on a separate dedicated network if desired. Security requirements apply to multiple networks if used.
9. Data transmission volumes and requirements must be clearly defined for normal and maximum levels.
10. Firewall configuration impact must be minimal and clearly defined.

# Where does the Data Security Team fit?

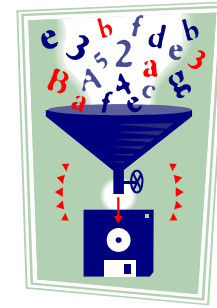


# Data Security

- Team of International SEMATECH Member Companies, Tool Suppliers, and Solution Providers.
- Charter: Given what data will be available to be shared, determine how to adequately and realistically protect the data and associated intellectual property exchanged as a result of e-diagnostics, while enabling the gains of e-Diagnostics for both suppliers and manufacturers.
- Scope:
  - Classification of Data Security
  - Classification of authorization levels and escalation procedures for higher-level access
  - Security associated with granting activities, i.e., remote control, s/w update, ...
  - Data disposal (how, not when)



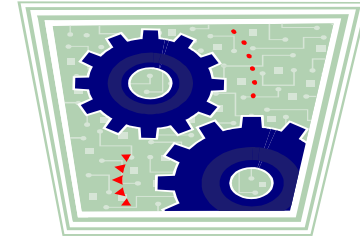
# Data Classification



All e-Diagnostics data is classified for security. The range of classification is as follows (from lowest to highest):

- 0 Unrestricted/Public: data that have little to no proprietary value (i.e., power quality)
1. Confidential/Restricted: where data had a larger audience than Secret/Confidential but access was limited to the specific scope that the data was associated with.
2. Secret/Confidential: where data is not as restricted as Top Secret/Private but generally the audience was a bit larger.
3. Top Secret/Private: where data is limited to a specific audience and/or dissemination or movement of this data is severely limited.

# Summary



- Security has been addressed early in the project
- Guidelines are in place to steer progress towards workable solutions

