Security Planning Rubric

The grid below describes the status of issues that districts can examine to determine current degree of security preparedness.

Management	Basic	Developing	Adequate	Advanced
District Administrative Leadership				
Security Goals	Provides minimal direction and oversight on IT related security issues to stakeholders and district leadership. Acknowledges efforts made by CTO to meet governing security and confidentiality requirements.	Develops a basic mission statement on security that is shared and acted upon by IT department. Authorizes CTO to ensure compliance with governing security and confidentiality regulations.	Articulates a clear mission statement on security with stakeholders and district leadership. Authorizes CTO and security team to ensure compliance with governing security and confidentiality regulations. Is periodically involved in high level security planning.	Articulates a clear mission statement on security that is integrated with District policy and overall mission. Authorizes CTO and security team to ensure compliance with governing security and confidentiality regulations. Regularly provides oversight of high level security planning.
Legal Compliance	Initial effort has been made to bring IT installations into compliance with security-related laws (FERPA, CIPA, HIPPA, etc.), but actual level of compliance is not clear.	IT unit manages compliance with governing security-related laws (FERPA, CIPA, HIPPA, etc), as far as major vulnerably are concerned: (content, filtering, confidential databases.)	Security team assists with identifying potential concerns for compliance with all State and Federal Laws (FERPA, CIPA, HIPPA, electronic discovery, etc.). IT unit makes such compliance part of its protocol for new installations and periodic security reviews.	Security team or external auditor verifies full compliance with all State and Federal Laws (FERPA, CIPA. HIPPA, electronic discovery, etc.) Compliance review is routine component of new installations and periodic review.
Policy Implementation	District policy governing security efforts is limited to general statements that may be challenging to translate into specific security measures.	District policy governing security efforts provides a basic sense of direction for implementing security. Some policy areas may be missing (e.g. enforcement procedures for security violations.)	District policy governing security efforts provides adequate direction for implementing security measures. Some policy area out of date or lack clarity. District leaders specifically authorize the IT unit to enforce policy.	District policy governing security efforts provides effective direction with sufficient clarity to ensure appropriate implementation. District leaders specifically authorize IT unit to enforce policy. Security Team provides additional oversight.
Budget, Human Resources	No support specifically earmarked for security.	"Security" is not a budget line item, but some purchasing reflects security needs.	Key security-related items including personnel, hardware, software, etc included in budget planning.	Key security-related items including personnel, hardware, software, etc included in budget planning.
Communications	Little or no leadership communication on security issues to district leaders, board members, etc (stakeholders).	Leadership occasionally delivers security message to stakeholders.	Leadership regularly delivers clear message to stakeholders. Is periodically involved in high level security planning.	Leadership effectively and frequently incorporates security message into stake holder communication when appropriate.

	Basic	Developing	Adequate	Advanced
Security Team				
Charter Responsibilities	No formal team exists.	Ad hoc security team lacks formal authorization.	Security team is authorized by the district administrators to develop a security plan and oversee its implementation.	Security team is authorized by the school board/committee to develop a security plan and oversee its implementation.
Membership	No formal security team exists. IT Staff and district leadership confer on security requirements on an ad hoc basis.	Ad hoc Security team members include representatives from: Teacher or administrator. IT staff	Security team members include representatives from: District Administration, School Board, or community Teaching staff, IT staff, Legal Staff and HR .	Security team members include: Superintendent, School Board member, Teaching staff, IT staff, Legal staff, HR, law enforcement and community representative.
General Incidence Response	No clearly defined procedures in place for incidence response.	Have procedure in place for reporting security issues.	Clear procedures in place that include how to report a security breach and steps for response.	Clearly documented procedures in place that include how to report and document security issues, and steps for response and follow up.
Ransomware Incidence Response	No clearly defined procedures in place for ransomware preparation or response.	Have procedure in place for ransomware preparation.	Clear procedures in place that include how to prepare for a ransomware incident and steps for response.	Clear procedures in place that include how to prepare for a ransomware incident and steps for response.

	Basic	Developing	Adequate	Advanced
Security Planning				
IT Planning in General	Little or no planning.	IT planning includes some consideration of security.	IT planning includes security as a component. Security provisions included in contracts with vendors, consultant, and outsourced services are reviewed for compliance with District security requirements.	IT planning fully integrates security requirements. Security provisions included in contracts with vendors, consultants, and outsources services are reviewed for compliance with District security requirements. District general security planning is fully coordinated with IT security planning.
Security Plan	Security practices exist without a formal security plan. Security plan does not address communication with stakeholders or community in case of an incident Security plan includes occasional testing and monitoring.	Security plan exists as an internal IT department document. Security plan includes limited communication with stakeholders in case of an incident. Security Plan includes occasional testing and monitoring.	Security plan written or reviewed in past 24 months. Security plan includes communication with stakeholders in case of an incident. Security Plan is derived from asset-based risk assessment process and includes end- user training and communication and periodic testing and monitoring.	Security plan revised or reviewed in past 12 months and discussed and approved by district leadership and school board. The security plan includes communication with stakeholders and community in case of an incident. Security plan is derived from asset-based risk assessment process, is comprehensive: plan links district goals and policies, end- user training and communication and includes periodic testing and monitoring.
Security Audit	No security audit for technical vulnerabilities, assessment for systems holding sensitive data; review of security policies completed within the past 36 months	Internal security audit completed within the past 36 months. Scope of audit linked to security plan.	Internal security audit completed within the past 18 months. Scope of audit linked to security plan. District provides budget support for security measures.	Security plan is derived from asset-based risk assessment process, is comprehensive: plan links district goals and policies, end- user training and communication and includes periodic testing and monitoring.
Security Penetration Testing	No penetration testing	Penetration testing completed within the past 36 months.	Penetration testing completed within the past 18 months	Security plan is derived from asset-based risk assessment process, is comprehensive: plan links district goals and policies, end- user training and communication and includes periodic testing and monitoring.

	Basic	Developing	Adequate	Advanced
Security Implementation				
Staff Competency	IT staff insufficiently trained in desktop support or network management.	Job description indicates mixed network and desktop support roles without specific mention of security-related tasks.	Clear division of responsibility between network and desktop support, with clear assignment of responsibility for security tasks and roles.	Clear division of responsibilities, including security-related tasks. Additionally, IT staff is cross-trained to provide backup support.
Staffing Levels	Technology staffing is insufficient to provide basic IT support services. Critical service interruptions affecting the entire district or individual schools last days or weeks.	Dedicated IT staff exists, but in insufficient numbers to provide basic IT support services. Staff responds and resolves technology service interruptions affecting the entire district or an entire school within two working days.	Dedicated IT staff exists and provides functional IT support services. Staff responds and resolves technology service interruptions affecting the entire district or an entire school within the same working day. Problems affecting a single classroom are resolved within two working days.	Full time dedicated IT staff. Responds and resolves critical technology incidents on the same day they are reported. Minor incidents are resolved by the next business day. IT systems operate at a high level of reliability due to effective organizational practices.
Security Staffing	No one specifically assigned to attend to security.	CTO or other management staff also deals with security.	A staff person is assigned to manage security. The security officer reports to the CTO	A Chief Security Officer exists. The security officer reports outside IT department

Technology	Basic	Developing	Adequate	Advanced
Perimeter Defense				
Overview	Architecture at basic stage; shortcomings exist in all areas.	Architecture lacks capacity for growth or implementation of stronger security measures; shortcomings exist in two or more areas.	Architecture lacks capacity for growth or implementation of stronger security measures; shortcomings exist in two or more areas.	Appropriate Architecture with room to grow.
DMZ	Computer host or small network inserted as a 'neutral zone' between a district's private network and the outside public network.			
	DMZ: building servers double as firewalls (no DMZ).	Firewall in place but no DMZ to protect email and web servers.	DMZ, firewall, VPN services exist but may be inadequate for future growth.	DMZ, firewall, VPN configured for appropriate external access, email and web services.
Firewall	Firewall software not present at all network entry points.	Perimeter /intrusion defense: installed, firewall configured and monitored.	Perimeter/intrusion defense: fully configured, firewall configured and monitored.	Perimeter / intrusion defense: a layered strategy from desktop to firewall provides fully integrated protection.
VPN - Network access for remote users	No VPN configured.	No VPN or insufficient VPN controls.	VPN permits a limited number of users to access the network remotely.	VPN configured to provide secure access to all authorized remoter users.
Virus Protection	Virus protection is not installed on all network-connected devices. Virus definition updates are performed sporadically.	Virus protection installed on all devices; centrally –managed updates for at least half of client computers; all other computers	Centrally managed, integrated virus protection. Firewall, intrusion detection is deployed to most end points.	Centrally managed, integrated virus protection, firewall, intrusion detection for all end points.
Wireless Access Control	Wireless Access: Reliance on end-user caution or light, localized usage to limit risk.	Wireless access may be spreading faster than it can be properly controlled. Not all access points are properly	Wireless access is properly configured. Secondary strategies may include non-technical tactics (e.g. powering off access points over weekends).	Wireless access properly configured; secondary strategies (VPN, segmentation) provide risks are minimized by monitoring and strong authentication control.
IPS - Intrusion Prevention System	No IPS configured	IPS is configured sporadically. IPS is not fully functioning.	IPS is configured and monitoring critical IPS is properly configured and fully facilities such as network segments	
Content Filtering	Web filtering has been implemented to meet the requirements of local policy, state laws, and federal laws.	Web filter logs are reviewed regularly to note use and determine adjustments in categories.	Users can request modifications to web filter blocking for school use; requests are reviewed and action taken within 48 hours of request.	School employees have overrides to web filter for school purposes.

	Basic	Developing	Adequate	Advanced
LAN Management				
Backups	Backups may not include all mission critical servers.	Daily and weekly backups. Off-site storage not established.	Consistent backups including off-site storage; periodically tested.	Consistent backups including off-site routinely tested. File restoration practice included in crisis management preparedness and ransomware response.
Routine Network Monitoring & Testing	Minimally scheduled network checks. No file integrity testing. No capacity for password testing.	Daily checks for virus protection, network serviced, backup status. No file integrity testing. No capacity for District-wide password testing.	Daily checks for network intrusion, virus protection, network series, backup status. Monthly file integrity testing. Password testing every 60-90 days.	Live monitoring for network intrusion, virus protection. Daily checks on network services, backup status. Maintenance logs kept. Monthly file integrity testing. .Password testing every 60-90 days. Twice-yearly wireless network intrusion detection.
Major Systems Maintenance	Major services (email, internet access) occasionally unavailable for 8 hours or more.	Major services (email, internet access) rarely unavailable for 8 hours or more.	Major services (email, internet access) rarely unavailable for more than 4 hours.	Major services (email, internet access) rarely unavailable for more than 2 hours.
Redundancy	Servers may lack RAID (computer data storage schemes that can divide and replicate data among multiple disk drives) reliability; no spare parts on hand for critical network devices.	Some critical district servers have RAID reliability; some spare parts on hand.	Most critical servers are protected by redundant units. Spare components may not be available for all critical network devices.	All critical servers are protected by redundant units. Spare components are available for all critical network devices.
Documentation	No daily maintenance and monitoring logs. System documentation is largely absent. Equipment inventory managed at the building level.	Maintenance logs kept. System documentation is minimal; knowledge of system configuration is highly dependent on individuals. Client end point inventory managed at building level; all network components	Maintenance logs kept. System documentation is maintained for critical services and network management. Client end point inventory managed at district level.	Maintenance logs kept. System documentation is maintained for all services and network management. Client end point inventory managed at district level.
External Partners and Vendors	External partners' or vendors' security practices are not known or verified.	External partners' or vendors' security practices: documentation exists but practices are not verified.	External partners' or vendors' security practices: vendors assert that federal, state, and district requirements are met. Vendor credentials are checked. Emergency procedures for service restoration are established.	External partners' or vendors' security practices: external audit reports verify that federal, state and district requirements are met. Redundant systems are in place; emergency procedures for service
Encryption	Encryption is implemented sporadically on the network, or not at all.	Passwords are encrypted in transit and in storage on centralized servers and applications. Wireless networks are encrypted with shared keys.	All interfaces (web, file transfer, etc.) to applications containing student, employee and financial data are encrypted. Passwords are encrypted in transit and in storage on centralized servers and applications. Wireless	All student, employee and financial data subject to regulatory compliance requirements is encrypted in storage and in transit. Passwords to all centralized applications are encrypted in storage and in transit.

	Basic	Developing	Adequate	Advanced
WAN Security				
Segmentation	Splitting a network into subnetworks, for improved performance, increased security and containing network problems.			
	Segmentation: no network segmentation beyond building-level.	Segmentation: no network segmentation beyond building-level.	Segmentation: network appropriately segmented.	Segmentation: centrally-managed building LANs, switches, servers.
Authentication/ Authorization	Authentication /Authorization: not available.	Authentication/ Authorization: not managed via the WAN, if at all. End users have no access beyond local LANs to WAN resources (except to specific systems).	Authentication/Authorization: system-wide implementation may be incomplete.	Authentication/Authorization: deployed throughout the district.
Multipath	No multipath internet access.	No multipath internet access.	Multipath internet access available for critical functions.	Multipath internet access available
Standardization	Building LANs not standardized, require local maintenance.	Building LANs not standardized, require local maintenance.	Most but not all building LANs, switches, servers support remote management.	Standardized hardware and network configuration throughout district.
Remote LAN Management	WAN lacks remote monitoring and management of routers, switched and LAN servers.	Existing WAN devices may not support remote monitoring and management. As WAN expands, new devices will support remote management; legacy devices may remain in service past "retirement" age.	IT plan includes elimination of legacy devices that cannot be remotely managed.	All routers, switches and LAN servers are remotely monitored and managed.
Patch Management	Servers, other networks devices: sporadic. End Point Devices: virus data and system updates (patch management) are the responsibility of the end user. Classroom or lab computers: desktop management software may be in use for updates in a few locations.	Servers, other network devices: routine updates. End Point Devices: IT unit provides instructions and reminders for virus data file and system updates (patch management) to end users whose computers are not automatically updated. Classroom or lab computers: central IT staff use desktop management software for updates in some locations.	Servers, other network devices: automated updates. End Point Devices: most virus data and system updates (patch management) are managed remotely for most computers. Classroom and lab computers: central IT staff have established efficient protocols to refresh operating systems and deploy software in many locations.	Server, other network devices: automated updates. End Point Devices: all virus data and system updates (patch management) are managed remotely. Classroom and lab computers: central IT staff have established efficient protocols to refresh operating systems and deploy software in all locations.
Software Licensing	Software licensing managed at the building level	Software licensing for operating systems, virus protection and office productivity software is site-licensed by central IT group; other software, purchased without central guidance or controlling policy is controlled at the building level.	Software licensing for operating systems, virus protection and office productivity software is site-licensed by IT group; other software is purchased with central guidance	Software licensing for operating systems, virus protection and office productivity software is site licensed by central IT group; other software is purchased with central guidance or controlling policy to coordinate training and encourage shareable knowledge and increased cost savings. There is a procedure to self-audit licenses at district locations

	Basic	Developing	Adequate	Advanced
Point Security				
Installation, Configuration, Repair of desktop computers	Client desktop computers: no remote management. No capacity to rebuild computers using imaging software.	Client desktop computers: mixed local and central responsibilities. Some computers can be rebuilt using imaging software.	Client desktop computers: strong central policy, distributed management. Most computers can be rebuilt using imaging software.	Client desktop computers: strong central policy, distributed management. Maximized efficient repairs using imaging software.
Standardization	No standardization plan exists. Any defacto standard for hardware and software result from episodic bulk purchasing and or donations. No cycle of hardware replacement exists.	Legacy software and hardware hampers standardization efforts. No cycle of hardware replacement exists. Typically four or five generations of both PCs and Macs may be on line.	Legacy software and hardware are in the process of being phased out. 5 to 6 year replacement cycle established. Number of operating systems supported has been reduced to 2, Mac and PC.	Standardization goals are achieved. 3-4 year replacement cycle established. The majority of all computers use one operating system.
Passwords	Password protection is end users responsibility; periodic password changes are not required.	Password policies exist by are not centrally enforced nor routinely used in all locations.	Password policy is monitored by LAN or WAN managers.	Central password policy including periodic password changes, is monitored and enforced by WAN managers.
Advanced User Security	Simple password log in is all that required to access most areas of the network	Password log in is required and there are some areas of network not accessible for all users	Strong password requirements are in place for at-risk locations, databases, or systems	Two factor authentication are in place on all computers and other end points.

	Basic	Developing	Adequate	Advanced
Cloud Security				
Security Responsibilities	Contract does not delineate division of responsibility between district and CSP	Contract does not delineate division of responsibility between district and CSP	Contract delineates some of the division of responsibility between district and CSP but there may be gaps	Contract delineates full division of responsibility between district and CSP
Contract	Contract and SLA do not include Event logging and notification DDOS protection Availability requirements Intrusion detection and prevention Data ownership	Contract or SLA includes some of Event logging and notification DDOS protection Availability requirements Intrusion detection and prevention Data ownership	Contract or SLA includes Event logging and notification DDOS protection Availability requirements Intrusion detection and prevention Data ownership	Contract or SLA includes Event logging and notification DDOS protection Availability requirements Intrusion detection and prevention Data ownership
Egress	Contract does not specify what happens with data when the district concludes their contract	Contract specifies that data is returned to the district when the district concludes their contract.	Contract specifies that data is returned to the district and wiped everywhere when the district concludes their contract.	Contract specifies that data is returned to the district and wiped everywhere when the district concludes their contract.

Business Continuity	Basic	Developing	Adequate	Advanced
Crisis Management Plan	Disaster Recovery Planning is the process that requires detailed planning and preparation prior to an event – whether man made or natural, and then setting the groundwork for understanding the process of responding and recovery. IT Crisis Management plan identifying Mitigation/Prevention, Preparedness, Response, and Recovery does not yet exist. Staff has not been trained specifically for IT crisis management. District Crisis Management plan includes few if any references to technology or IT security.	IT Crisis Management plan has been outlined; it may have been completed more than a year earlier and has not been updated. Staff training for crises has been minimal. District Crisis Management Plan includes brief references to IT and security issues.	IT Crisis Management plan uses same asset-based model as the security plan; it includes details of major systems. The plan may have been completed more than a year earlier and has not been updated. The plan includes an inventory of required equipment.	IT Crisis Management plan uses the same asset-based model as the security plan; it includes details of all systems from ISP to desktop. Plan is reviewed and updated every 12 months. The plan includes an inventory of required equipment redundancy and facilities for hot site requirements.
Crisis Management Training	No plan in place to train personnel for crisis situations.	Personnel trained for crisis situations, no simulations conducted.	Personnel trained for crisis situations, simulations conducted to test Business Continuity Plan when developed.	Personnel trained for crisis situations, simulations conducted from shut down to start up to assess Business Continuity Plan on an annual basis.
Technology Asset Inventory	No plan exists for critical components to maintain or restore services in the event of a natural or man-made crisis.	Acceptable levels of service needs during the recovery period of a crisis have been determined to identify what processes need to be maintained or restored first to keep the school running.	A technology asset inventory has been completed to determine and document the mission-critical technology	A technology asset inventory has been completed to determine and document the mission-critical technology components, their location, how they're configured, and who is responsible for management. Essential employees and other critical partners (vendors, sub-contractors, services, logistics, etc.) required to maintain business operations by location and function during the event have been identified. Critical backup are in place for both equipment and staff.

Environmental Safety	Basic	Developing	Adequate	Advanced
Anticipation of Natural Disasters	Flood or water damage: network devices may be in basements or sitting on floors.	Flood or water damage: network devices may be in basements or sitting on floors.	Flood or water damage: critical infrastructure not at risk.	Flood or water damage: critical infrastructure not at risk. Redundant equipment and warning systems are in place to guard against other disasters.
Fire Protection	Fire: No dedicated alarms. Network equipment may be located in unlocked, multi-use spaces (offices, classrooms, etc. No fire suppression system in place.	Fire: No dedicated alarms. Network equipment may be located in space also used for storage or custodial purposes. No cooling or fire suppression systems in place.	Fire: Alarms installed, Network equipment in clean, dedicated space. Cooling systems and fire suppression systems in place.	Fire: Alarms and suppression equipment installed. Network equipment in clean, dedicated space.
Climate Control	Temperature and humidity: no dedicated HVAC for network services.	Temperature and humidity: network devices may lack protection from extreme heat, dampness.	Temperature and humidity: network devices properly ventilated.	Temperature and humidity: network devices properly ventilated.
Power Supply	Power: minimal UPS support for servers.	Power: most servers & network devices on UPS.	Power: all servers & network devices protected by uninterruptable power supply units.	Power: all servers & network devices protected by UPS units with backup power available.
Inspection Review	No special environmental inspections are made.	Facilities are inspected occasionally for hazards.	Facilities are inspected occasionally for hazards.	Facilities and emergency equipment are inspected on regular basis by external experts.

Physical Security	Basic	Developing	Adequate	Advanced
Facilities	Many network devices are in shared or uncontrolled locations, e.g. book cupboards, custodial closets. Network cabling may be exposed, within reach, or subject to damage during routine building cleaning and maintenance.	Most network devices in dedicated, secure locations. Network cabling may be exposed, within reach, or subject to damage during routine building cleaning and maintenance.	All network devices are in dedicated, secure locations. Most network cabling is secure.	All network devices are in dedicated secure spaces. All network cabling is secure.
End User Equipment	Not all equipment is physically secured where required.	Not all equipment is physically secured where required.	Most equipment is physically secured (locks, cables) where required.	All equipment is physically secured (locks, cables) where required. Equipment selection criteria include physical durability.

End Users	Basic	Developing	Adequate	Advanced
Awareness	Stakeholders generally lack expertise on, and awareness of security issues.	*Expertise:* Leaders may lack experience on strategic technology planning, including security issues. *Awareness:* Users are generally aware of organizational security concerns but lack specific knowledge on what to do.	*Expertise:* Those charged with oversight of IT attend some trainings on strategic and managerial topics. *Awareness:* Users are generally aware of essential security guidelines and follow some security procedures.	*Expertise:* District leaders demonstrate competency and knowledge of strategic and managerial IT topics, including security. *Awareness:* Users integrate essential security practices into everyday use of technology.
Training	Limited training opportunities do not include security topics. *District leaders* : Often choose not to participate in IT training. *End Users* : Training not required. *Community:* Little or no training available.	Security is mentioned in IT training and professional development but training is not consistently tied to security policy. *District leaders* : Occasionally participate in IT training. *End Users:* Not all are trained. *Community:* Occasional awareness and outreach sessions are offered to the community.	Security integrated into IT training and professional development. *District leaders* : Receive same IT training as all users. *End users* : Most are trained. *Community* : Periodic security awareness workshops are offered to the community.	Security integrated in IT training and professional development. *District leaders* : Receive regular user training, plus training on strategic IT topics. *End Users* : Professional development, including security training, is tied to district mission and security requirements. *Community* : Security is integrated into outreach programs.
Access Control	Control of student access to computers depends on direct supervision. Staff access to network devices is not restricted.	Student access to computers is appropriately controlled in some locations. Staff access to network devices is restricted in some locations.	Student access to computers is appropriately monitored where required. Staff access to network devices is restricted where appropriate.	Student access to computers is appropriately controlled and remotely monitored where required. Staff access to network devices is restricted where appropriate.
Communication	IT unit communicates to stakeholders only sporadically.	IT unit communicates to stakeholders a few times per year. *Leadership* : Received regular updates on IT and security issues. *End Users* : Receive occasional message issued on security concerns. *Community* : Received occasional publicity on IT or security issues.	IT unit updates stakeholders on organizational security concerns on a monthly basis, or more frequently if significant vulnerabilities arise. *Leadership* : Receives regular updates on IT and security issues. *End Users*: Messages issued on security concerns are disseminated using a variety of media at appropriate intervals to engage users. *Community* : Receives regular publicity on IT or security issues.	IT unit updates stakeholders on organizational security concerns on a monthly basis, or more frequently if significant vulnerabilities arise. *Leadership* : Receives regular updates on IT and security issues. *End Users* : Messages issued on security concerns are disseminated using a variety of media at appropriate intervals to engage users. *Community* : Recurring outreach to the community includes IT advice, security awareness.
Feedback	No organized feedback mechanisms exist.	Limited effort made to track stakeholder opinion and satisfaction.	Help desk tracks problems and suggestions.	Help desk tracks problems and suggestions.

			IT unit relies on stakeholders to bring complaints and suggestions forward.	Survey of user opinions may be performed every other year. All new IT initiatives including changes in security policy are reviewed by user groups.	Survey of user opinions performed yearly. Users provide input to IT initiatives through organized means such as special interest groups or regularly scheduled meetings.
	Summary: Community of Trust	IT unit almost no capacity to monitor security. IT systems are extremely vulnerable to internal damage.	Increasing likelihood for security failures- without clear policy or secure infrastructure – may result in a climate of suspicion or confusion.	Decreasing likelihood for security failures – the result of clear policy and significantly improved infrastructure – reduces lingering suspicion and confusion.	A secure network with reliable infrastructure and transparent security policies, provides effective, mission-driven learning opportunities without the weight of surveillance.