



District Security Planning Grid (rubric)

Management		Basic	Developing	Adequate	Advanced
District Leadership					
Oversight	Security Goals	-- provides minimal direction and oversight on IT-related security issues. -- acknowledges efforts made by IT Director to meet governing security and confidentiality regulations.	-- develops a basic mission statement on security. -- authorizes IT Director to ensure compliance with governing security and confidentiality regulations.	-- articulates a clear mission statement on security. -- authorizes IT Director 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 IT Director 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, HIPAA, etc.), but actual level of compliance is not clear.	IT unit manages compliance with governing security-related laws (FERPA, CIPA, HIPAA, etc.) as far as major vulnerabilities are concerned (content filtering, confidential databases)	Security team assists with identifying potential concerns for compliance with all State and Federal Laws (FERPA, CIPA, HIPAA, 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, HIPAA, etc.). -- Compliance review is a routine component of new installations and periodic reviews.
	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 -- Some policy areas out of date or lack clarity.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.
Support	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 included in budget planning.	Strong needs integrated into all IT budgeting.
	Communication	Little or no leadership communication on security issues.	Leadership occasionally delivers security messages to stakeholders.	Leadership regularly delivers clear message to stakeholders.	Leadership effectively and frequently incorporates security message in to stakeholder communication when appropriate.



Management, cont.		Basic	Developing	Adequate	Advanced
IT Security Management					
Security Team	Charter / Responsibilities	No formal security 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 includes: -- teacher or administrator -- IT staff	Security Team members include representatives from: -- District Administration -- School Board or community -- teaching staff -- IT staff	Security Team members include: -- Superintendent -- School Board member -- teacher -- IT director & key staff -- community representatives
Security Planning	IT Planning in general	Little or no IT planning.	IT planning includes some consideration of security.	-- IT planning includes security as a component. -- Security provisions included in contracts with vendors, consultants, 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 outsourced 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 -- Occasional testing and monitoring	-- Security plan exists as an internal IT department document. -- Includes occasional testing and monitoring.	-- Security plan written or reviewed in past 24 months -- Plan is derived from asset-based risk assessment process and: -- includes end-user training and communication -- includes periodic testing and monitoring.	-- Security plan revised or reviewed in past 12 months and discussed and approved by district leadership and school board. The Plan: -- is derived from asset-based risk assessment process; -- is comprehensive: plan links District goals and policies, end-user training and communication; -- includes periodic testing and monitoring.



Management, cont.		Basic	Developing	Adequate	Advanced
IT Security Management					
Security Planning	Security Audit	-- No security audit completed within past 36 months.	-- Internal security audit completed within past 36 months. -- Scope of audit linked to security plan (above).	-- Internal security audit completed within past 18 months. -- Scope of audit linked to security plan (above). -- District provides budget support for security measures.	-- Security audit completed by independent consulting group within past 18 months; internal audit completed within past 12 months. -- Scope of audit governed by comprehensive security plan.
	Crisis Management Plan	IT Crisis Management plan does not yet exist. -- Staff have 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 the 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. -- The plan includes an inventory of required equipment redundancy and facilities for hot site redundancy. -- The plan includes training and communication requirements.
Security Implementation	IT Staffing Levels	-- More than 750 computers per technical support staff person. -- Insufficient numbers to expand IT services. -- IT staff may be non-dedicated or part-time.	Full-time staff. Staff/computer ratio approximately 1:750.	staff to computer ratio: 1:500.	-- Staff to computer ratio: 1:250. -- IT systems operate at a high level of reliability due to effective organizational practices: further reduction in staff-to-equipment ratios may produce only slight improvement in service levels.
	Staff competency	-- Insufficiently trained in desktop support or network management.	-- Job descriptions indicate 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 are cross-trained to provide backup support.
	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	A Chief Security Officer exists



Technology	Basic	Developing	Adequate	Advanced
Architecture				
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:	Appropriate Architecture: solid functionality exists, but compared with advanced level, shortcomings exist in one or more areas:	Appropriate Architecture with room to grow.
DMZ	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.	Perimeter/intrusion defense: fully configured.	Perimeter/intrusion defense: a layered strategy from desktop to firewall provides fully integrated protection.
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 receive regular, manual updates.	Centrally managed, integrated virus protection -- firewall, intrusion detection is deployed to most workstations.	Centrally managed, integrated virus protection, firewall, intrusion detection for all workstations.
Content filtering / Spam control	Content filtering may have been implemented at some locations, but implementation is not monitored appropriately.	Content filtering has been implemented for all locations, but monitoring is sporadic.	Content filtering is properly monitored for effectiveness, but impact on throughput is unknown.	Content filtering is handled with devices capable of delivering a high level of effectiveness without significantly impacting network performance.
VPN	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 remote users.
Wireless Access control	<i>Wireless Access:</i> Reliance on end-user caution or light, localized usage to limit risk.	<i>Wireless access</i> may be spreading faster than it can be properly controlled. Not all access points are properly configured.	<i>Wireless access</i> is properly configured; Secondary strategies may include non-technical tactics (e.g. powering off access points over weekends). Intrusion risks are balanced against accessibility.	<i>Wireless access</i> properly configured; secondary strategies (VPN, segmentation) provide additional layer of security. Intrusion risks are minimized by monitoring and strong authentication control

Perimeter Defense



Technology, cont.		Basic	Developing	Adequate	Advanced
Architecture, continued					
WAN Security	Extent of Implementation	<i>Extent:</i> No district-wide WAN or less than half of schools on WAN.	<i>Extent:</i> majority of district schools on WAN.	<i>Extent:</i> all district schools on WAN. .	<i>Extent:</i> all district schools on WAN.
	Segmentation	<i>Segmentation :</i> no network segmentation beyond building-level.	<i>Segmentation:</i> no network segmentation beyond building-level.	<i>Segmentation :</i> network appropriately segmented.	<i>Segmentation :</i> centrally-managed building LANs, switches, servers.
	Authentication Authorization	<i>Authentication/authorization:</i> not available	<i>Authentication/authorization:</i> Not managed via the WAN, if at all. End users have no access beyond local LANs to WAN resources (except to specific systems).	<i>Authentication/authorization:</i> system-wide implementation may be incomplete	<i>Authentication/authorization:</i> deployed throughout district
	Redundancy	<i>Redundancy :</i> servers may lack RAID 5 reliability; no spare parts on hand for critical network devices.	<i>Redundancy:</i> critical district servers have RAID 5 reliability; some spare parts on hand.	<i>Redundancy :</i> most critical servers are protected by redundant units. Spare components may not be available for all critical network devices.	<i>Redundancy:</i> all critical servers are protected by redundant units. Spare components are available for all critical network devices.
	Standardization	<i>Standardization:</i> Building LANs not standardized, require local maintenance.	<i>Standardization:</i> Building LANs not standardized, require local maintenance.	<i>Standardization:</i> Most but not all building LANs, switches, servers support remote management.	<i>Standardization:</i> standardized hardware, network configuration.
	Remote WAN Management	<i>Remote Management:</i> WAN lacks remote monitoring and management of routers, switches and LAN servers.	<i>Remote Management:</i> 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.	<i>Remote Management:</i> IT Plan includes elimination of legacy devices that cannot be remotely managed.	<i>Remote Management:</i> All routers, switches and LAN servers are remotely monitored and managed.
Internet	Bandwidth	<i>Bandwidth:</i> dial-up, cable, or DSL occasionally creates bottleneck.	<i>Bandwidth :</i> cable, DSL, frame relay, or T1: network usually reliable, although bandwidth may be inadequate for growing use.	<i>Bandwidth:</i> adequate for current requirements but may lack capacity for future expansion.	<i>Bandwidth :</i> adequate for current requirements, expandable for future growth.
	Internet Infrastructure	no redundant internet access.	no redundant internet access.	backup internet access on line (cable, DSL) for critical functions.	Backup internet access on line (cable, DSL) for critical functions.



Technology, cont.		Basic	Developing	Adequate	Advanced
IT Operations -- WAN & LAN management					
LAN Management	Overview	<u>Firefighting Mode</u> Most time spent on urgent problems	<u>Growing pains</u> IT operations include time allocated for some monitoring and maintenance	<u>Standards and procedures in place</u> IT operations include time allocated for routine monitoring and maintenance.	<u>Efficient, growth-oriented operation</u> IT operations include time allocated for routine monitoring and maintenance.
	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.
	Routine Network Monitoring & Testing	-- Minimal scheduled network checks. -- No file integrity testing. -- No capacity for password testing	-- Daily checks for virus protection, network services, backup status. -- No file integrity testing. -- No capacity for District-wide password testing.	-- Daily checks for network intrusion, virus protection, network services, 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.
	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 computer inventory managed at building level; all network components managed by central IT group.	-- Maintenance logs kept. -- System documentation is maintained for critical services and network management. -- Client computer inventory managed at district level;	-- Maintenance logs kept. -- System documentation is maintained for all services and network management. -- Client computer inventory managed at district level
	External Partners & 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 restoration are established. If required, all code is escrowed.



Technology, cont.		Basic	Developing	Adequate	Advanced
IT Operations -- End User Security					
End User Security	Overview	<u>Unenforceable, not verifiable</u> Workstation policies and protocols at the user level are non-existent or haphazardly enforced.	<u>Increasing, not verifiable</u> Workstation policies and protocols not adequate to support organizational IT security goals.	<u>Widely in use, generally verifiable</u> Workstation policies and protocols at the user level assist organizational security with appropriate hardware and software controls.	<u>Seamless, highly verifiable</u> Workstation policies and protocols at the user level assist organizational security with appropriate hardware and software controls.
	Installation, configuration, repair	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. -- maximally efficient repairs using imaging software.
	Standardization	No standardization plan exists. Any de facto standards for hardware and software result from episodic bulk purchasing 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	Standardization goals are achieved. -- 3 to 4 year replacement cycle established. -- The majority of all computers use one operating system.
	Patch management and application updates (network & end user)	-- Servers, other network devices: sporadic. -- Teacher/administrator computers: 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. -- Teacher/administrator computers: 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. -- Teacher/administrator computers: 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.	-- Servers, other network devices: automated updates. -- Teacher/administrator computers: 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 central 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.
	Passwords	Password protection is end users' responsibility; periodic password changes are not required.	Password policies exist but are not centrally enforced nor routinely used in all locations.	Password policy is monitored by LAN or WAN managers.	Central password policy is monitored and enforced by WAN managers.
	Advanced End User Security			Strong password requirements are in place for at-risk locations, databases, or systems.	For large districts, biometric security devices, smartcards, or strong password requirements are in place on all computers.



Environmental & Physical Security

Basic	Developing	Adequate	Advanced
-------	------------	----------	----------

Environmental Security				
Environmental Security: overview	<u>Environmental hazards given cursory attention:</u>	<u>Environmental hazards partly addressed:</u>	<u>Most environmental hazards addressed.</u>	<u>Environmental hazards recognized and addressed.</u>
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.).	Fire: no dedicated alarms. Network equipment may be located in space also used for storage or custodial purposes.	Fire: alarms installed. Network equipment in clean, dedicated space.	Fire: alarms and suppression equipment installed. Network equipment in clean, dedicated space.
Climate Control	Temperature and humidity: no dedicated HVAC for network devices .	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 uninterruptible 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 periodically for most hazards	Facilities and emergency equipment are inspected on regular basis by external experts.

Physical Security				
Overview	<u>IT facilities and infrastructure: not secure.</u>	<u>IT facilities and infrastructure: partially secure.</u>	<u>IT facilities and infrastructure: mostly secure.</u>	<u>IT facilities and infrastructure: secure.</u>
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 are 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 space. -- All network cabling is secure.
End User equipment security	-- Not all equipment is not 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.
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.



End Users	Basic	Developing	Adequate	Advanced
End User Security	<p>Awareness</p> <p>-- Stakeholders generally lack expertise on and awareness of security issues.</p>	<p><i>Expertise: District leaders often less capable than many teachers in the use of productivity tools.</i></p> <p><i>--Leaders may lack experience on strategic technology planning, including security issues.</i></p> <p><i>Awareness: Users are generally aware of organizational security concerns but lack specific knowledge on what to do.</i></p>	<p><i>Expertise: District leaders demonstrate use of productivity tools.</i></p> <p><i>-- Those charged with oversight of IT attend some trainings on strategic and managerial topics.</i></p> <p><i>Awareness: Users are generally aware of essential security guidelines and follow some security procedures.</i></p>	<p><i>Expertise: District leaders demonstrate competency with productivity tools and knowledge of strategic and managerial IT topics, including security.</i></p> <p><i>Awareness: Users integrate essential security practices into everyday use of technology.</i></p>
	<p>Training</p> <p>Limited training opportunities do not include security topics.</p> <p>-- <i>District leaders: often choose not to participate in IT training.</i></p> <p>-- <i>End Users: training not required.</i></p> <p>-- <i>Community: little or no training available</i></p>	<p>Security is mentioned in IT training and professional development but training is not consistently tied to security policy.</p> <p>-- <i>District leaders: occasionally participate in IT training.</i></p> <p>-- <i>End Users: Not all are trained.</i></p> <p>-- <i>Community: occasional awareness and outreach sessions are offered to the community.</i></p>	<p>Security integrated into IT training and professional development.</p> <p>-- <i>District leaders: receive same IT training as all users.</i></p> <p>-- <i>End Users: Most are trained.</i></p> <p>-- <i>Community: Seasonal or periodic security awareness workshops are offered to the community.</i></p>	<p>Security integrated into IT training and professional development.</p> <p>-- <i>District leaders: receive regular user training plus training on strategic IT topics.</i></p> <p>-- <i>End Users: Professional development, including security training, is tied to district mission and security requirements.</i></p> <p>-- <i>Community: Security is integrated into all outreach.</i></p>
	<p>Communication</p> <p>IT unit communicates to stakeholders only sporadically.</p> <p>-- <i>Leadership: receives periodic updates on IT and security issues.</i></p> <p>-- <i>End Users: receive only sporadic messages issued on security concerns.</i></p> <p>-- <i>Community: receives infrequent publicity on IT or security issues</i></p>	<p>IT unit communicates to stakeholders a few times per year.</p> <p>-- <i>Leadership: receives regular updates on IT and security issues.</i></p> <p>-- <i>End Users: receive occasional messages issued on security concerns.</i></p> <p>-- <i>Community: receives occasional publicity on IT or security issues</i></p>	<p>IT unit updates stakeholders on organizational security concerns on a monthly basis, or more frequently if significant vulnerabilities arise.</p> <p>-- <i>Leadership: receives regular updates on IT and security issues.</i></p> <p>-- <i>End Users: frequent messages issued on security concerns are disseminated using a variety of media</i></p> <p>-- <i>Community: receives regular publicity on IT or security issues.</i></p>	<p>IT unit updates stakeholders on organizational security concerns on a monthly basis, or more frequently if significant vulnerabilities arise.</p> <p>-- <i>Leadership: receives regular updates on IT and security issues.</i></p> <p>-- <i>End Users: frequent messages issued on security concerns are disseminated using a variety of media</i></p> <p>-- <i>Community: recurring outreach to the community includes IT advice, security awareness.</i></p>



End Users, cont.		Basic	Developing	Adequate	Advanced
End User Security	Feedback	No organized feedback mechanisms exist.	Limited effort made to track stakeholder opinion and satisfaction. IT Unit relies on stakeholders to bring complaints and suggestions forward.	Help desk tracks problems and suggestions. Survey of user opinions may be performed every other year. All new IT initiatives including changes in security policy are reviewed by user groups.	Help desk tracks problems and suggestions. 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 has 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. -- Early adopters of new technology may be frustrated by apparent unresponsiveness of IT unit to meet their needs.	Decreasing likelihood for security failures - the result of clear policy and significantly improved infrastructure-- reduces lingering suspicion and confusion. -- Early adopters of new technology learn to collaborate with IT unit to ensure security while promoting innovation.	A secure network, with reliable infrastructure and transparent security policies, provides effective, mission-driven learning opportunities without the weight of surveillance.

