01

Governance sets the rules for every security decision

The foundation is risk-based classification, lifecycle accountability and documented approval.

01	APPLY	Use the directives across planning, design, construction, commissioning, operation, upgrades and decommissioning.
02	CLASSIFY	Establish business criteria, Facility Security Classification and a Security Risk Assessment before selecting controls.
03	CONTROL	Use approved service providers, follow staged submissions, and manage waivers, confidentiality and environmental constraints.
04	EVIDENCE	The Facility Operator owns compliance, closes inspection findings and maintains Proof of Compliance for SAIS review.

Source: SAIS 2017 Security Directives • SEC-01 • Executive summary; consult the approved directive for compliance.

02

The perimeter is a layered delay-and-detection system

Fence selection is not standalone—it must integrate barriers, clear zones, sensing, surveillance and lighting.

CATEGORY

Select the applicable fencing category from facility classification and risk; address shared, internal, construction and property fences.

DELAY

Provide structural strength, forced-entry resistance, durable fabric, anti-climb features and anti-vehicle protection.

DETECT

Coordinate intrusion sensors, fixed and assessment cameras, long-range surveillance and perimeter lighting.

DETAIL

Engineer clearances, terrain profiles, penetrations, grounding, post installation and emergency gates; submit compliance evidence.

Source: SAIS 2017 Security Directives • SEC-02 • Executive summary; consult the approved directive for compliance.

03

A gate must inspect, control and contain

A compliant gate manages the full journey of people and vehicles without losing containment.

01

APPROACH

Use a preliminary checkpoint and vehicle approach-speed management before the secure boundary.

02

INSPECT

Provide gatehouse, inspection/rejection areas, X-ray or screening spaces and overwatch where required.

03

AUTHORIZE

Separate vehicle, pedestrian, visitor and support flows; integrate access control, communications and surveillance.

04

CONTAIN

Use rated barriers, response zones, clearances, resilient power and controlled arrangements for unmanned or emergency gates.

Source: SAIS 2017 Security Directives • SEC-03 • Executive summary; consult the approved directive for compliance.

04

Lighting must make detection dependable

Uniform, camera-compatible illumination is a security control—not simply a facilities service.

23 lux
at fence line ±1 m

20 lux
3 m inside

12 lux
10 m outside

UNIFORMITY	Maintain overlapping illumination, a maximum 6:1 light-to-dark ratio and at least 70% of camera field of view illuminated.
APPLICATIONS	Design perimeter, area, checkpoint, gatehouse-interior and shared-fence lighting for their distinct tasks.
ENGINEERING	Validate point-by-point calculations; coordinate poles, luminaires, cabling, controls, backup power and maintenance.
COMPATIBILITY	Avoid glare, blind spots or interference with cameras and intrusion sensors; increase levels where surveillance requires it.

Source: SAIS 2017 Security Directives • SEC-04 • Executive summary; consult the approved directive for compliance.

05

Security systems converge at the control center

Individual technologies become effective only when integrated into one monitored operating environment.

01	SENSE	Deploy access control, license plate recognition, intrusion detection and assessment, identity management and video surveillance as required.
02	DESIGN	Meet environmental, network, cybersecurity, power, storage and system-availability constraints.
03	INTEGRATE	Correlate alarms, video and identity events; interface required plant-control functions without weakening segregation.
04	OPERATE	Centralize monitoring and response in the Security Control Center, with documented application and Proof of Compliance.

Source: SAIS 2017 Security Directives • SEC-05 • Executive summary; consult the approved directive for compliance.

06

Security devices require certified performance

Selection must be tied to recognized certification, operational performance and the threat being controlled.

INSPECTION

Specify certified X-ray, explosive-trace, walk-through metal detection and under-vehicle inspection systems.

PROTECTION

Provide ballistic vests, helmets and resistant glazing where the risk and post require personnel protection.

DETERRENCE

Use raise-arm barriers, turnstiles and crash-rated anti-vehicle barriers for controlled movement and containment.

ASSURANCE

Document ratings, testing, environmental suitability, integration, training and maintenance in the compliance package.

Source: SAIS 2017 Security Directives • SEC-06 • Executive summary; consult the approved directive for compliance.

07

Security power is designed for uninterrupted operation

Continuity comes from layered sources, automatic transfer, conditioning, UPS coverage and monitored recovery.

01

NORMAL

Feed security loads from reliable essential utility power, correctly sized for all systems and infrastructure.

02

ALTERNATE

Provide an alternate feed with automatic transfer; a one-second delay filters brief transients.

03

BACKUP

If both feeds fail, start the dedicated generator after five seconds and restore supply within 30 seconds.

04

BRIDGE

Use UPS, grounding, surge/lightning protection, failure annunciation and tested maintenance to preserve operation and settings.

Source: SAIS 2017 Security Directives • SEC-07 • Executive summary; consult the approved directive for compliance.

08

Communications must be secure, segregated and resilient

Voice, data and video services need protected paths for security, fire and emergency response.

01	WIRED	Provide always-ready hotlines and fiber-based infrastructure linking gates, checkpoints, government forces and the control center.
02	WIRELESS	Engineer radio coverage, secure mobile communications and field services for reliable operational coordination.
03	NETWORK	Use a dedicated security network with encryption, controlled access, protected equipment, redundancy and cybersecurity controls.
04	SUSTAIN	Back communications with compliant power, preventive maintenance, support arrangements and current configuration records.

Source: SAIS 2017 Security Directives • SEC-08 • Executive summary; consult the approved directive for compliance.

09

Security equipment needs a hardened home

Rooms, cabinets, doors and locks form part of the protective system—not just its enclosure.

Level III

ballistic protection

205 mm

wall options

2 systems

independent A/C

STRUCTURE	Use secured rooms or dedicated structures with structural, electrical and environmental safeguards; exclude windows from equipment areas.
ACCESS	Restrict entry through compliant steel doors and controlled locking/key systems to authorized personnel.
FIELD CABINETS	Place cabinets inside the secure perimeter; provide tamper alarms, weather sealing, suitable locks and temperature-rated equipment.
CONTROL CENTER	Protect the Security Control Center while supporting safe, ergonomic and maintainable operation.

Source: SAIS 2017 Security Directives • SEC-09 • Executive summary; consult the approved directive for compliance.

Railway penetration becomes a managed security operation

The train's movement through the perimeter must be governed by a site-specific Railway Security Operation Plan.

01

PLAN

Base the RSOP on the facility risk assessment and define responsibilities, operating rules and security interfaces.

02

CROSS

Protect the perimeter opening, track alignment and adjacent security systems while the train enters and exits.

03

VERIFY

Control rolling stock, seals, inspections, chain of custody and hazardous-material movements.

04

COORDINATE

Align the operator, facility, government forces and responders through communications and emergency plans.

Source: SAIS 2017 Security Directives • SEC-10 • Executive summary; consult the approved directive for compliance.

11

PIV cards establish trusted identity through their full lifecycle

Trust depends on verified issuance, tamper resistance, protected data and prompt revocation—not appearance alone.

01	PROOF	Issue cards only after identity verification and Facility Operator authorization; define validity and revocation processes.
02	CARD	Use standards-based physical stock, bilingual printed data, photograph, signature and visual anti-counterfeit cues.
03	DIGITAL	Protect machine-readable elements with encryption, controlled keys, PINs and biometrics where required.
04	LIFECYCLE	Manage issuance, personalization, activation, renewal, loss, suspension, revocation, return and audit records.

Source: SAIS 2017 Security Directives • SEC-11 • Executive summary; consult the approved directive for compliance.

Cybersecurity is continuous governance plus technical control

Security and industrial-control assets require a managed cycle of risk, protection, response and recovery.

GOVERN

Maintain measurable cybersecurity policy, accountable ownership and annual—or post-incident—management review.

ASSESS

Identify critical assets, perform risk assessment and penetration testing, treat findings and validate through annual external audit.

PROTECT

Enforce network boundaries, controlled external connections, secure remote access, account management, training and physical safeguards.

RECOVER

Operate incident response, backup and recovery, configuration/change control, data protection and secure media disposal.

Source: SAIS 2017 Security Directives • SEC-12 • Executive summary; consult the approved directive for compliance.

Marine interfaces extend the security perimeter onto the water

Coastal, port and offshore facilities need marine-rated technology plus coordinated waterside detection and response.

1,000 m

marine-interface zone

3 types

coastal • port • offshore

Integrated

detection + response

HARDEN	Use corrosion-resistant, sealed devices and accelerated maintenance where salt spray affects security equipment.
ASSESS	Address the Marine Interface Area in the risk assessment and establish a dedicated marine-security function.
CONTROL	Define access, exclusion zones, barriers, alarms, imaging, intrusion detection and patrol requirements.
COORDINATE	Provide boats and communications as needed; align procedures with the Coast Guard and other government agencies.

Source: SAIS 2017 Security Directives • SEC-13 • Executive summary; consult the approved directive for compliance.

Security projects move through four controlled approval stages

Early risk decisions must remain traceable through design, construction, testing and operational readiness.

01

SRA + CONCEPT

Define risks, classification, conceptual security architecture and the basis of design.

02

PRELIMINARY

Develop coordinated layouts, system concepts, equipment strategy and initial compliance evidence.

03

DETAIL

Submit complete drawings, calculations, specifications, data sheets and directive-by-directive compliance.

04

READINESS

Complete construction inspection, site acceptance, documentation, training and operational-readiness certification.

Source: SAIS 2017 Security Directives • SEC-14 • Executive summary; consult the approved directive for compliance.

15

Operations require a documented security management system

People, procedures, maintenance and assurance must sustain the facility's security posture over its full lifecycle.

01	ACCOUNTABILITY	Assign ownership; maintain the risk assessment, Facility Security Plan, operating procedures and Industrial Security Department.
02	PEOPLE	Control staffing, competence, training, weapons, transport and construction-to-startup security arrangements.
03	READINESS	Maintain fences, power, lighting, screening and security systems; apply safe work and management-of-change controls.
04	ASSURANCE	Report and investigate incidents, exercise emergency plans, conduct audits and retain Proof of Compliance documentation.

Source: SAIS 2017 Security Directives • SEC-15 • Executive summary; consult the approved directive for compliance.

16

Pipeline protection follows risk along the entire corridor

The security plan must cover exposed lines, critical nodes, rights-of-way and the response capability between sites.

01

ASSESS

Evaluate existing and new pipelines, with special focus on pumping stations, scraper facilities and isolated valves.

02

ASSIGN

Define ownership and responsibilities for operations, maintenance and security across each pipeline and corridor.

03

WATCH

Control fence penetrations and patrol the full route using personnel or suitable imaging; fence and monitor urban sections.

04

RESPOND

Coordinate an event response plan and maintain the pipeline, right-of-way, vegetation, access and security equipment.

Source: SAIS 2017 Security Directives • SEC-16 • Executive summary; consult the approved directive for compliance.

17

Substations are secured by functional classification

Business criticality and site risk establish the Functional Classification—and therefore the security baseline.

BCA + SRA

classification basis

3Q

annual TSR submission

Site-specific

uplift and waivers

CLASSIFY	Assign each substation a Functional Classification using Business Criteria Analysis and Security Risk Assessment.
STANDARDIZE	Use approved Typical Security Requirements for repeatable designs, while retaining site-specific assessment.
APPROVE	Class 1–3 substations at industrial facilities follow normal approval stages; other locations may use the approved annual TSR.
ADAPT	Increase controls for border or elevated-risk sites and resolve justified constraints through formal waivers before construction.

Source: SAIS 2017 Security Directives • SEC-17 • Executive summary; consult the approved directive for compliance.

Industrial cities need coordinated perimeter and access governance

The designated authority secures the city boundary while each autonomous facility retains its own compliance duties.

GOVERNANCE

Complete a city-level risk assessment, define authority responsibilities and keep each tenant facility on the normal workflow.

PERIMETER

Use at least Category 4 fencing, compliant penetrations, video assessment and long-range intrusion detection.

ACCESS

Cover every entrance lane with license-plate recognition; manage access with compliant systems and PIV credentials.

OPERATIONS

Use traffic studies to size employee, visitor/contractor and truck gates; operate an integrated city Security Control Center.

Source: SAIS 2017 Security Directives • SEC-18 • Executive summary; consult the approved directive for compliance.

19

Residential compounds need separation and controlled access

Residential protection begins with safe siting, then layers perimeter, gate, surveillance and operating controls.

01	SEPARATE	Locate the compound outside the industrial operating perimeter and establish spacing using the applicable safety directive.
02	BOUNDARY	Use rigid welded mesh or solid walls, anti-climb topping and a maintained six-metre clear zone on both sides.
03	GATES	Provide ballistic gatehouse protection, rated anti-vehicle barriers, speed management, rejection/inspection flow and auxiliary access.
04	OPERATE	Integrate lighting, surveillance, access control, communications, fire protection, procedures and Proof of Compliance.

Source: SAIS 2017 Security Directives • SEC-19 • Executive summary; consult the approved directive for compliance.