الوحدة 2

مقدمة حول أمن ومرونة البنية الأساسية الحرجة

OFFICE OF ANTITERRORISM ASSISTANCE

هدف الوحدة

- في نهاية هذه الوحدة التعليمية، سيتمكن المشاركون من وصف أهمية تطبيق نظام جيد التصميم للحماية المادية بغرض تأمين المنشآت الحيوية بالبنية الأساسية الحرجة.

Module Objective

- By the end of this module, you will be able to describe the importance of implementing a well-designed physical protection system for the security of critical infrastructure

البنية الأساسية الحرجة

- الأنظمة والأصول، المادية أو المعنوية، ذات الأهمية الحيوية للبلاد بحيث أن تعطيلها أو تدميرها من شأنه أن يلحق ضررا فائقا في المجالات التالية:
  - الأمن
  - أمن الإقتصاد الوطني
  - الصحة أو السلامة العامة في البلاد
  - أي مزيج من العوامل السابقة

Critical Infrastructure

- Systems and assets, whether physical or virtual, so vital to the nation that the incapacity or destruction of such systems and assets would have a debilitating impact on:
  - Security
  - National economic security
  - National public health or safety
  - Any combination of those matters

الأمن

- تطبيق مجموعة إجراءات وتدابير يتعين اتخاذها بجملتها بغرض تغيير معدل وقوع الأحداث غير المرغوبة بالنسبة لإجمالي الحدث بناءً على:
  - المخاطر التي تم تحديدها
  - التهديدات
  - الثغرات الأمنية
  - إحتمالية وقوع أحداث غير مرغوبة

Security

- The implementation of a set of procedures and processes that when taken as a whole have the effect of altering the ratio of undesirable events to total event based on:
  - Identified risks
  - Threats
  - Vulnerabilities
  - Probability of an undesirable occurrence

الحاجة إلى الأمن

- حماية الأرواح والممتلكات
- الحفاظ على الأصول الحرجة
- الحفاظ على الإستقرار السياسي والاقتصادي

Need for Security

- Protect lives and property
- Sustain critical assets
- Maintain political and economic stability

بناء الشراكات المجتمعية

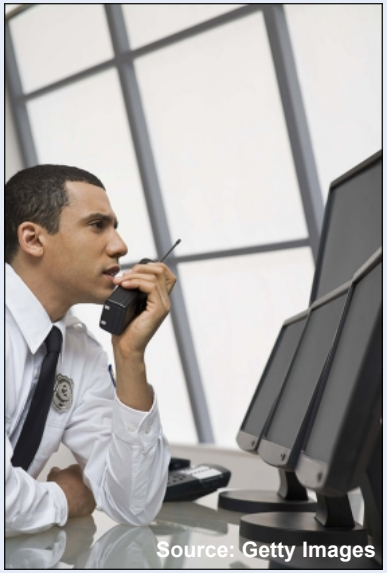
- لحماية وضمان مرونة البنية الأساسية الحرجة يتعين بناء شراكات مع عدة جهات مختلفة:
  - الحكومة
  - القطاع الخاص
  - القطاع الأكاديمي والإحترافي
  - بعض المنظمات الخيرية والتطوعية الخاصة

Building Community Partnerships

- Protecting and ensuring the resilience of critical infrastructure requires partnerships with multiple entities:
  - Government
  - Private sector
  - Academic and professional
  - Certain not-for-profit and private volunteer organizations

نظرة عامة على الوعي بالرصد

- إجراء أمني دفاعي
- ملاحظة وكشف والتبليغ عن المراقبة المعادية
- ضروري للغاية لحماية البنية الأساسية الحرجة
- يُستخدم في عمليات الأمن السيبراني


Source: Getty Images

Surveillance Awareness Overview

- A defensive security operation
- Observe, detect, and report hostile surveillance
- Crucial to protection of critical infrastructures
- Used in cyber security operations

نقاط الضعف

- سمات مادية أو صفات عملياتية من شأنها تعريض منشأة أو مرفق للإستغلال أو لتهديد معين

Vulnerability

- A physical feature or operational attribute that renders an entity open to exploitation or susceptible to given threat

تحليل نقاط الضعف

- منتج أو عملية تحديد السمات المادية أو العملياتية التي تُعرِّض للخطر أية مرافق أو أصول أو أنظمة أو شبكات أو مناطق جغرافية أو لأية تهديدات محيقة

Vulnerability Analysis

- A product or process of identifying physical features or operational attributes that renders an entity, asset, system, network, or geographic area susceptible or exposed to threats

سؤال للمناقشة

- ما هي بعض الأمثلة للمشاكل الأمنية الخاصة بالبنية الأساسية الحرجة التي قد تحتاج لمعالجتها؟

Discussion Question

- What are some examples of critical infrastructure security problems you may need to address?

هدف تحليل نقاط الضعف

- قيّم فعالية التدابير الأمنية المضادة التي تم تطبيقها
- حافظ على الموارد المحدودة
- استمر في توفير معلومات دقيقة لمسؤولي الأمن دعما لاتخاذ القرار

Vulnerability Analysis Purpose

- Evaluate the effectiveness of implemented security countermeasures
- Preserve limited resources
- Provide security managers with accurate information in support of security decision making

لحظة التعليم الإسترجاعي

- ماهو الغرض من إجراء تحليل نقاط الضعف بالبنية الأساسية الحرجة؟

TeachBack Moment

- What is the purpose of conducting a critical infrastructure vulnerability analysis?

تعريف نظام الحماية المادية

- نظام يجمع بين الأفراد والسياسات والإجراءات والمعدات بغرض حماية الأصول أو المنشآت من كافة التهديدات

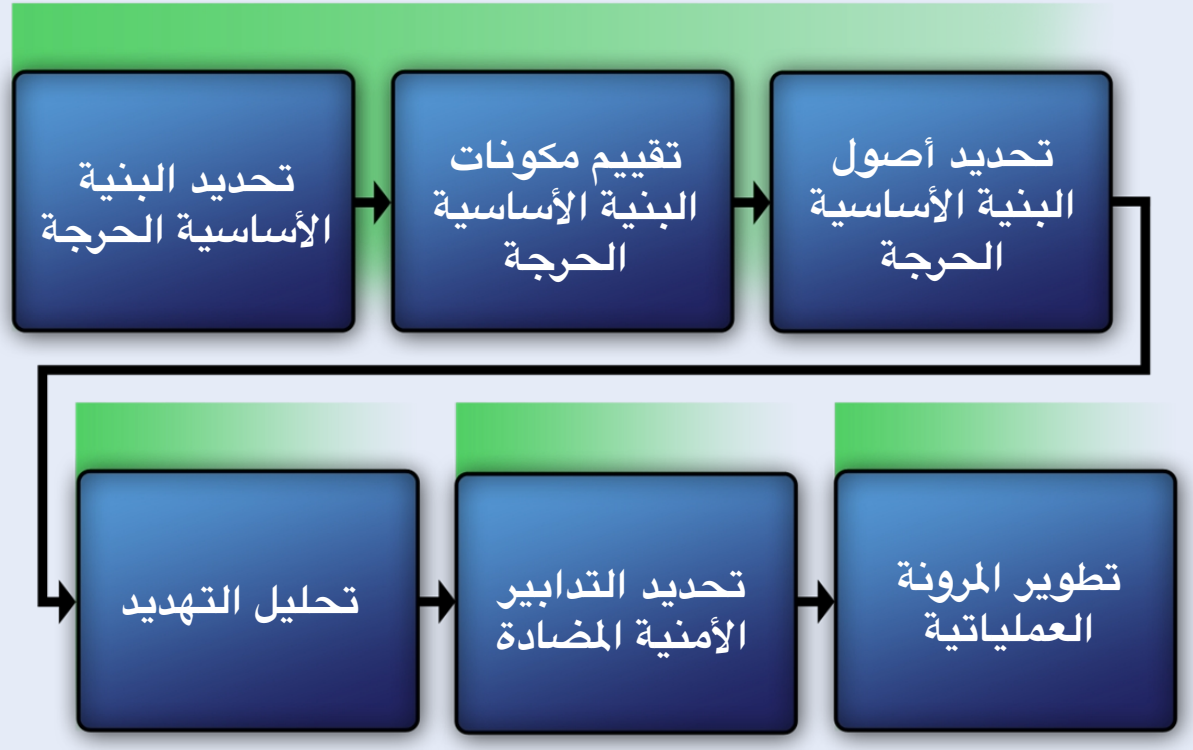
Physical Protection System Definition

- An integration of people, policies and procedures, and equipment for the protection of assets or facilities against all threats

الرسم البياني الخاص بنظام الحماية المادية

راجع

الكتيب 2.1



Physical Protection System Diagram		Refer To: Workbook 2.1
Identify Critical Infrastructure	Assess Critical Infrastructure Components	Identify Critical Infrastructure Assets
Analyze the Threat	Identify Security Counter-measures	Develop Operational Resilience

مكونات نظام الحماية المادية

راجع

الكتيب 2.1

- يبدأ تصميم وتنفيذ نظام الحماية المادية الفعال بتحليل نقاط الضعف.

Physical Protection System Components	Refer To: Workbook 2.1

- Design and implementation of an effective physical protection system begins with vulnerability analysis

الخطوة 1: تحديد البنية الأساسية الحرجة

راجع

الكتيب 2.1

- تحديد البنية الأساسية الحرجة لتقييم أية تدابير أمنية مضادة ذات صلة

Step 1: Identify Critical Infrastructure	Refer To: Workbook 2.1

- Identify critical infrastructure to assess any associated security countermeasures

فئات البنية الأساسية الحرجة

راجع

الكتيب 2.1

- ما هي بعض فئات البنية الأساسية الحرجة؟

Critical Infrastructure Categories	Refer To:
	Workbook 2.1

- What are some categories of critical infrastructure?

الخطوة 2: تقييم مكونات البنية الأساسية الحرجة

راجع

الكتيب 2.1

- الظروف البيئية
- الظروف المادية
- عمليات المنشأة
- السياسات والإجراءات الخاصة بالمنشأة
- المتطلبات التنظيمية
- اعتبارات السلامة

Step 2: Assess Critical Infrastructure Components	Refer To: Workbook 2.1
▪ Environmental conditions ▪ Physical conditions ▪ Facility operations ▪ Facility policies and procedures ▪ Regulatory requirements ▪ Safety considerations	

هدف تقييم مكونات البنية الأساسية الحرجة

- ترتيب أولويات الجهود
- استخدام الموارد المحدودة بكفاءة
- تنفيذ التدابير الأمنية المضادة في أهم المنشآت الحيوية

Purpose of Critical Infrastructure Component Assessment

- Prioritize efforts
- Use limited resources more efficiently
- Implement security countermeasures on the most important facilities

الخطوة 3: تحديد أصول البنية الأساسية الحرجة

راجع

الكتيب 2.1

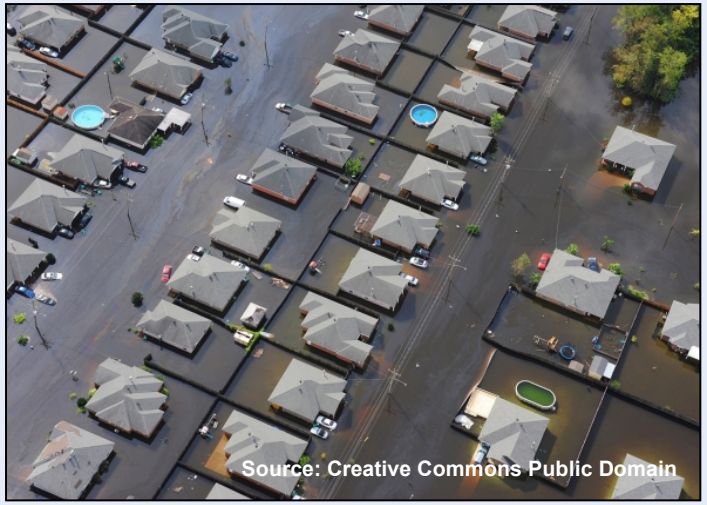
- تندرج الأصول الحرجة عادة تحت واحدة من أربع فئات:
  - الأشخاص
  - المعلومات
  - الإجراءات
  - المعدات (التكنولوجيا)

Step 3: Identify Critical Infrastructure Assets	Refer To: Workbook 2.1

- Critical assets typically are in one of four categories:
  - People
  - Information
  - Processes
  - Equipment (technology)

ترتيب أولويات أصول البنية الأساسية الحرجة

- تحديد التهديدات
- تحديد التبعات غير المرغوب فيها للخسائر
- تحديد إحتمالية الحدوث



Prioritize
Critical Infrastructure Assets

- Identify threats
- Specify undesirable consequences of loss
- Determine the probability of occurrence

تحديد التهديدات

- التخريب
- الإعتداء
- إعاقة العمليات
- الهجوم السيبري
- عدم التوافر
- الخسارة أو السرقة
- التنازلات
- الإتلاف

Identify Threats

- Nonavailability
- Loss or theft
- Compromise
- Destruction
- Sabotage
- Assault
- Impaired operations
- Cyberattack

العواقب غير المرغوب فيها للخسارة

- حدد العواقب غير المرغوب فيها للخسارة في كل أصل
- حدد قيمة كل عاقبة تم تحديدها:
  - منخفضة
  - متوسطة
  - عالية

Undesirable Consequences of Loss

- For every asset specify all undesirable consequences of loss
- Assign values to each of the consequences specified:
  - Low
  - Medium
  - High

إحتمالية الحدوث

- تقييم احتمالية حدوث الهجوم عن طريق تحليل:
  - معلومات الاستخبارات
  - فعالية التدابير الأمنية المضادة القائمة
- وضع قيمة تقديرية لكل حادث محتمل: منخفضة، متوسطة، أو عالية

Probability of Occurrence

- Evaluate the probability of attack by analyzing:
  - Intelligence information
  - The effectiveness of existing security countermeasures
- Assign value of low, medium, or high to the probability

نشاط أصول البنية الأساسية الحرجة

راجع

راجع النشرة 2.1

- الغرض: هو التعرف على الأصول الحيوية الخاصة بمنشأة حكومية قياسية أو معيارية تُقل رئيس الدولة أو كبار الشخصيات
  - المدة: 20 دقيقة (15 للنشاط، 5 لاستخلاص المعلومات)
  - تركيبة المجموعة: مجموعات كل طاولة
  - استخلاص المعلومات: نقاش يدور في إطار مجموعة كبيرة

Critical Infrastructure Assets Activity	Refer To: Handout 2.1

- Purpose: to identify critical assets for a standard government facility that houses the Head of State or other dignitaries
  - Duration: 20 minutes (15-activity; 5-debrief)
  - Group composition: table groups
  - Debrief: large-group discussion

الخطوة 4: تحليل التهديد

راجع

الكتيب 2.1

- فحص خصائص التهديد
- تحديد صياغة المعلومات الواردة في بيان تحليل التهديد:
  - تلخيص المعلومات التي تم جمعها
  - تحديد التهديدات التي تواجه المنشأة
  - تقييم نظام الحماية المادية في البنية الأساسية

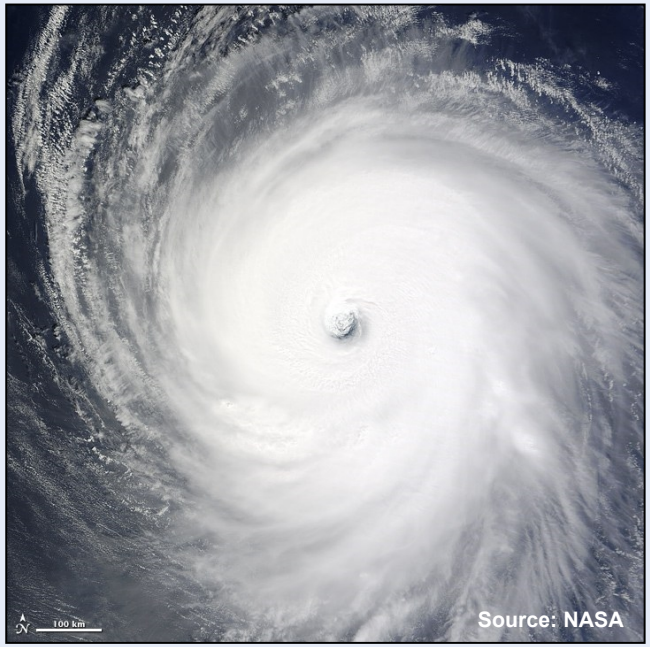
Step 4: Analyze the Threat

Refer To: Workbook 2.1

- Examine the characteristics of the threat
- Formalize the information in the threat analysis statement to:
  - Summarize gathered information
  - Identify facility threats
  - Evaluate an infrastructure's physical protection system

خصائص التهديد الواجب أخذها في الاعتبار في الكوارث الطبيعية

- قبل إعداد بيان تحليل التهديد، يتعين اعتبار العناصر التالية:
  - نوع الكارثة
  - التأثيرات المحتملة
  - المناطق المتضررة



Natural Disaster Threat Characteristics to Consider

- Before drafting the threat analysis statement, consider the following:
  - Type of disaster
  - Potential effects
  - Areas affected

أسئلة المناقشة

- ما هي التهديدات الناشئة من بعض الكوارث الطبيعية في منطقتك؟
- ما هي النتائج المحتملة؟

Discussion Questions

- What are some natural disaster threats in your area?
- What are the potential effects?

سمات التهديد الإرهابي التي ينبغي أخذها في الاعتبار

- قبل إعداد بيان تحليل التهديد، يتعين اعتبار التالي بالنسبة للعناصر الإرهابية:
  - الدوافع
  - نوع التهديدات
  - المعدات والأسلحة
  - التكتيكات

Source: Getty Images

Terrorist Threat
Characteristics to Consider

- Before drafting the threat analysis statement, consider the terrorists':
  - Motivations
  - Types of threats
  - Equipment and weapons
  - Tactics

سؤال للمناقشة

- ما هي أكثر أنواع التهديدات الإرهابية المحتمل وقوعها في منطقتك؟

Discussion Question

- Which types of terrorist threats are most likely in your region?

المعدات والأسلحة

- تساعد معرفة نطاق الأسلحة المحتمل استخدامها على تطبيق الإجراءات الأمنية المناسبة
- يستخدم الإرهابيون في العادة أجهزة متفجرة مرتجلة

Equipment and Weapons

- Knowing the range of possible weapons allows for implementation of appropriate security measures
- Terrorists typically use improvised explosive devices

التكتيكات الإرهابية

- القوة
- الخلسة
- الخداع

Terrorist Tactics

- Force
- Stealth
- Deceit

الخطوة 5: الفحص الأمني والتحقق

راجع

الكتيب 2.1

- تحديد وتقييم التدابير الأمنية المضادة:
  - الفعالية
  - توصيات للتحسين
- توفير معايير التقييم:
  - التحقق من كل تدبير أمني مضاد
  - تحديد فعالية نظام الحماية المادية القائم بصفة كلية

Step 5: Security Inspection and Validation	Refer To: Workbook 2.1

- Identify and evaluate security countermeasures:
  - Effectiveness
  - Recommendations for improvement
- Provide evaluation criteria:
  - Validate each security countermeasure
  - Determine overall effectiveness of existing physical protection system

التدابير الأمنية المضادة الفعالة

- يتعين أن تكون مصممة بحيث تحمي من أنواع ومستويات التهديدات التي يتم تحديدها أثناء تحليل التهديد

Effective Security Countermeasures

- Should be designed to protect against the types and level of threats identified during the threat analysis

تقييم التدابير الأمنية المضادة

- لتحديد الفعالية، يتعين تقييم العناصر التالية:
  - السياسات والإجراءات
  - القوة الأمنية
  - التكنولوجيا

Evaluate Security Countermeasures

- To determine effectiveness, assess the following elements:
  - Policies and procedures
    - Security force
    - Technology

السياسات والإجراءات

- يتعين التركيز على:
  - القوة الأمنية
  - التكنولوجيا

Source: DS/T/ATA

Policies and Procedures

- Should focus on:
  - Security force
  - Technology

السياسات والإجراءات الخاصة بالتدابير الأمنية المضادة (1 من 2)

- يجب أن تتضمن:
  - حواجز المحيط الأمني
  - الإضاءة
  - أنظمة كشف التسلل
  - الدائرة التلفزيونية المغلقة
  - الأنظمة الأوتوماتيكية للتحكم بالدخول

Policies and Procedures for Security Countermeasures (1 of 2)

- Should include:
  - Perimeter barriers
  - Lighting
  - Intruder detection systems
  - Closed-circuit television
  - Automated access control system

السياسات والإجراءات الخاصة بالتدابير الأمنية المضادة (2 من 2)

- ضباط الأمن والدوريات (القوة الأمنية)
- التحكم في الأقفال والمفاتيح
- نقاط التحكم في الدخول
- تأمين مواقع الأصول (المرافق والمنشآت)
- إدارة تهديدات القنابل
- تكنولوجيا المعلومات

Policies and Procedures for Security Countermeasures (2 of 2)

- Security officers and patrols (security force)
- Lock and key controls
- Entry control areas
- Secure asset locations
- Bomb threat management
- Information technology

هدف القوة الأمنية

- التدخل المباشر بطريقة فعالة لإيقاف وتحييد العمل الإرهابي وإصابة الإرهابيين بالشلل قبل تحقيق مأربهم

Security Force Purpose

- Effectively interrupt actions and neutralize terrorists or threats before they achieve their goal

عناصر القوة الأمنية

- تشمل العناصر التي تساهم في فعالية القوة الأمنية ما يلي:
  - انتقاء أفراد القوة الأمنية
  - التدريب الأولي والمستمر
  - نشر المعدات الكافية
  - الإشراف المناسب من مركز القيادة والسيطرة

Security Force Elements

- Elements that contribute to the effectiveness of a security force include:
  - Selection of security force members
  - Initial and continuous training
  - Deployment of adequate equipment
  - Appropriate supervision from command and control

فعالية القوة الأمنية

- تعتمد على:
  - القدرة على العمل في ظل السياسات والإجراءات القائمة
  - القدرة التكنولوجية على رصد وتقييم وتوفير التعطيل المناسب للعمليات الإرهابية

Security Force Effectiveness

- Depends on the:
  - Ability to operate within established policies and procedures
  - Capability of the technology to detect, assess, and provide adequate delay

الغرض من التكنولوجيا

- يتعين أن يقوم مدراء الأمن بالنظر في الحلول التقنية وغير التقنية التي من شأنها:
  - رصد العناصر الإرهابية المتسللة (أجهزة كشف التسلل)
  - تعطيل الإرهابيين عن التقدم صوب الهدف (العوائق)

Technology Purpose

- Security managers must consider technical and nontechnical solutions that will:
  - Detect terrorists or intruders (intrusion detection systems)
  - Delay terrorists from progressing towards the target (barriers)

عناصر التكنولوجيا

- أنظمة كشف التسلل
- الحواجز

Technology Elements

- Intrusion detection systems
- Barriers

الدعم التكنولوجي لزيادة فعالية نظام الحماية المادية

- الحماية العميقة
- الحد الأدنى لعواقب فشل أحد المكونات
- الحماية المتوازنة

Technology Supports
Physical Protection System Effectiveness

- Protection-in-depth
- Minimum consequences of component failure
- Balanced protection

الخطوة 6: تطوير المرونة العملياتية

راجع

الكتيب 2.1

- تنقيح وتوضيح العلاقات الوظيفية عبر الوكالات
- تمكين فعالية تبادل المعلومات
- تطبيق عمليات المدمج والتحليل الوظيفي لتوفير المعلومات التخطيطية

Step 6: Develop Operational Resilience	Refer To: Workbook 2.1

- Refine and clarify functional relationships across agencies
- Enable effective information exchange
- Implement an integration and analysis function to inform planning

لحظة التعليم الإسترجاعي

- ما هي مكونات نظام الحماية المادية؟

TeachBack Moment

- What are the components of a physical protection system?

توصيات النظام الأمني (1 من 3)

- تم وضع تلك التوصيات بناء على التالي:
  - اختبار أداء ذو مجال محدود: القيام باختبارات أداء محدودة النطاق تشمل فقط عناصر محددة من نظام الحماية المادية
  - تحليل الفجوة: تحديد الفجوة بين التدابير المضادة القائمة والمطلوبة

Security System
Recommendations (1 of 3)

- Developed as a result from:
  - Limited scope performance testing: conducting tests on specific elements of a physical protection system
  - Gap analysis: identifying the gap between existing and required countermeasures

توصيات النظام الأمني (2 من 3)

- الجدوى: تحديد ما إذا كان الحل المقترح مناسبا أو منطقيا
- المرونة: القدرة على الإعداد والتأقلم والتكيف مع الظروف المتغيرة والصمود والتعافي بسرعة من التعطيلات مثل الهجمات المتعمدة والوقائع أو التهديدات أو الحوادث الطبيعية

Security System
Recommendations (2 of 3)

- Feasibility: determining whether a solution is suitable or logical
- Resilience: the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions such as deliberate attacks, accidents, or naturally occurring threats or incidents

توصيات النظام الأمني (3 من 3)

- المسائلة: تحديد ما إذا كانت التدابير الأمنية المضادة المقترحة توفر الحماية المطلوبة وتقع داخل إطار الموارد المتاحة

Security System Recommendations (3 of 3)

- Acceptability: determining whether the recommended security countermeasure provides the required protection and falls within scope of available resources

وظائف نظام الحماية المادية

راجع

الكتيب 2.2

- الكشف والتقييم
- التعطيل (التأخير)
- الاستجابة

Physical Protection System Functions	Refer To: Workbook 2.2
▪ Detection and assessment ▪ Delay ▪ Response	

النشاط الخاص بوظائف نظام الحماية المادية

راجع

الكتيب 2.2

- الغرض: الإشارة إلى أية وظيفة من وظائف نظام الحماية المادية التي يصفها النشاط المحدد
  - المدة: 10 دقائق (5 للنشاط، 5 لاستخلاص المعلومات)
  - تركيبة المجموعة: مجموعات كل طاولة
  - استخلاص المعلومات: نقاش يدور في إطار مجموعة كبيرة

Physical Protection System Functions Activity	Refer To: Workbook 2.2

- Purpose: to indicate which function of a physical protection system a specified action describes
  - Duration: 10 minutes (5-activity; 5-debrief)
  - Group composition: table groups
  - Debrief: large-group discussion

الإعتماد المتبادل بين قطاعات البنية الأساسية الحرجة

- لا تقتصر البنية الأساسية الحرجة على أنظمة الأشغال العامة
- إعادة التعريف بغرض زيادة المستوى الأمني والوعي لردع الهجمات

Critical Infrastructure Interdependence

- Critical infrastructure is no longer limited to public works systems
- Redefined to increase security and awareness to deter attacks

أمثلة على التهديدات ونقاط الضعف

- المعرفة الضرورية:
  - ما هي العناصر الحرجة الواجب حمايتها
  - كيفية حماية كل عنصر حرج
- يتعين فهم طبيعة التهديدات ونقاط الضعف التي تواجه المسؤولين عن المرافق الحيوية للبنية الأساسية الحرجة في كل فئة أو قطاع

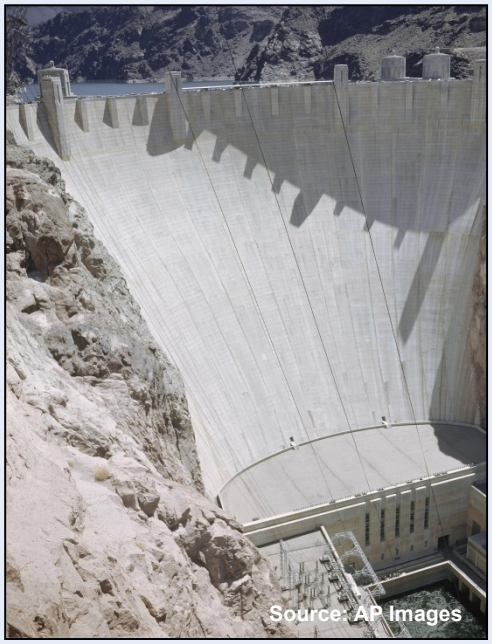
Examples, Threats, and Vulnerabilities

- Necessary knowledge:
  - Which critical elements to protect
  - How to protect each critical element
- Must understand the threats and vulnerabilities facing the managers of critical infrastructure, in each category or sector

فئات البنية الأساسية الحرجة (1 من 3)

راجع

راجع النشرة2.2



- الكيميائية
- المرافق التجارية
- الاتصالات
- تصنيع المواد الحرجة
- السدود

Critical Infrastructure Categories (1 of 3)	Refer To: Handout 2.2
▪ Chemical ▪ Commercial facilities ▪ Communications ▪ Critical manufacturing ▪ Dams	

فئات البنية الأساسية الحرجة (2 من 3)

راجع

راجع النشرة 2.2

- قاعدة الصناعات الدفاعية
- خدمات الطوارئ
- الطاقة
- الخدمات المالية
- الغذاء والزراعة
- المرافق الحكومية

Source: Stars and Stripes

Critical Infrastructure Categories (2 of 3)	Refer To: Handout 2.2
▪ Defense industrial base ▪ Emergency services ▪ Energy ▪ Financial services ▪ Food and agriculture ▪ Government facilities	

فئات البنية الأساسية الحرجة (3 من 3)

راجع

راجع النشرة 2.2

- الرعاية الصحية والصحة العامة
- تكنولوجيا المعلومات
- المفاعلات، والمواد، والنفايات النووية
- أنظمة النقل
- أنظمة المياه ومياه الصرف الصحي


Source: US Dept. of Transportation

Critical Infrastructure Categories (3 of 3)	Refer To: Handout 2.2

- Healthcare and public health
- Information technology
- Nuclear reactors, materials, and waste
- Transportation systems
- Water and wastewater systems

أسئلة المناقشة

- كيف يمكن مقارنة الإجابات السابقة على اللوح الورقي بقائمة الفئات المبينة؟
- ما هي بعض الأمثلة على البنية الأساسية الحرجة التي لا تحتويها هذه القائمة؟

Discussion Questions

- How do the earlier flip-chart responses compare with the list of categories shown?
- What are some examples of critical infrastructure that are not on this list?

نشاط فئات البنية الأساسية الحرجة

راجع

راجع النشرة2.3

- الغرض: التعرف على أمثلة محددة لكل من الفئات الـ 16 الخاصة بالبنية الأساسية الحرجة
  - المدة: 20 دقيقة (10 دقائق للنشاط، و 10 دقائق لاستخلاص المعلومات)
  - تركيبة المجموعة: مجموعات كل طاولة
  - استخلاص المعلومات: نقاش يدور في إطار مجموعة كبيرة

Critical Infrastructure Categories Activity	Refer To: Handout 2.3

- Purpose: to identify specific examples of each of the 16 critical infrastructure categories
  - Duration: 20 minutes (10-activity; 10-debrief)
  - Group composition: table groups
  - Debrief: large-group discussion

أسئلة المناقشة

- ما هي بعض الأمثلة للهجمات الإرهابية الأخيرة على البنية التحتية للنقل والمواصلات؟
- ما هي الهجمات السيبرانية الأخيرة التي عطلت مرافق البنية الأساسية الحرجة؟

Discussion Questions

- What are some examples of recent terrorist attacks on transportation infrastructure?
- What recent cyberattacks have disrupted critical infrastructure?

تعريف منهجية تحليل نقاط الضعف

- جرى العرف باستخدام المنهجيات التي ثبتت فعاليتها للتعرف على جوانب الضعف في البنية الأساسية الحرجة والتغلب عليها

Vulnerability Analysis Methodology Definition

- A proven approach used to identify and mitigate security weaknesses and vulnerabilities in an infrastructure

استخدام منهجية تحليل نقاط الضعف

- توفير المعلومات الضرورية بشأن:
  - اتخاذ تدابير مضادة لنقاط الضعف المحتملة
  - تقييم فعالية التدابير المضادة التي تم تطبيقها
  - عمل التغييرات اللازمة للتحسين

Vulnerability Analysis Methodology Use

- Provides the information necessary to:
  - Develop countermeasures for potential weaknesses
  - Evaluate the effectiveness of the countermeasures implemented
  - Make necessary changes for improvement

أربع مراحل لمنهجية تحليل نقاط الضعف (1 من 2)

راجع


الكتيب 2.3

- المرحلة 1:
  - تحديد البنية الأساسية الحرجة
  - تقييم مكونات البنية الأساسية الحرجة
  - تحديد أصول البنية الأساسية الحرجة
- المرحلة 2: تحليل التهديد بإجراء تحليل للتهديد وعمل توثيق كتابي لأنماط التهديد

Four Phases of Vulnerability Analysis Methodology (1 of 2)

Refer To: Workbook 2.3

- Phase 1:
  - Identify critical infrastructure
  - Assess critical infrastructure components
  - Identify critical infrastructure assets
- Phase 2: analyze the threat by conducting a threat analysis and providing written documentation of threat types

أربع مراحل لمنهجية تحليل نقاط الضعف (2 من 2)

راجع

الكتيب 2.3

- المرحلة 3: التعرف على التدابير الأمنية المضادة:
  - السياسات والإجراءات
  - القوة الأمنية
  - التكنولوجيا
- المرحلة 4: تطوير المرونة العملياتية:
  - تنفيذ عملية تحليل الفجوة
  - تحديد الإجراءات لإدارة التهديدات المحتملة

Four Phases of Vulnerability Analysis Methodology (2 of 2)

Refer To: Workbook 2.3

- Phase 3: identify security countermeasures:
  - Policies and procedures
  - Security force
  - Technology
- Phase 4: develop operational resilience:
  - Conduct a gap analysis
  - Determine actions to manage potential threats

لحظة التعليم الإسترجاعي

- ما هي أهمية المعلومات التي تم جمعها من خلال تحليل نقاط الضعف؟

TeachBack Moment

- What is the importance of the information collected during the vulnerability analysis?

تقرير نظام الحماية المادية

- المعلومات التي يجري جمعها من خلال تحليل نقاط الضعف يتم توثيقها في تقرير من شأنه:
  - تحديد نقاط الضعف
  - توفير فهم أفضل للأمن الخاص بنقاط الضعف
  - توفير التوصيات للتحسين
  - المساعدة في التخطيط للتدابير الأمنية المضادة وتنفيذها

Physical Protection System Report

- Information collected in a vulnerability analysis is documented in a report that:
  - Identifies weaknesses
  - Provides a better understanding of security vulnerabilities
  - Provides recommendations for improvement
  - Assists with planning and implementation of security countermeasures

عناصر تقرير نظام الحماية المادية (1 من 2)

- ملخص إداري
- مقدمة
- منهجية تحليل نقاط الضعف
- تعريف البنية الأساسية الحرجة
- تحليل مكونات البنية الأساسية الحرجة

Source: Getty Images

Elements of a Physical Protection System Report (1 of 2)

- Executive summary
- Introduction
- Vulnerability analysis methodology
- Critical infrastructure identification
- Critical infrastructure component analysis

عناصر تقرير نظام الحماية المادية (2 من 2)

- تعريف التهديد
- تقييم نظام الحماية المادية
- متطلبات اختبارات الأداء
- توصيات للتحسين
- الإستنتاجات المستخلصة
- المراجع

Elements of a Physical Protection System Report (2 of 2)

- Threat definition
- Physical protection system evaluation
- Performance testing requirements
- Recommendations for improvements
- Conclusions
- References

مناقشة تقرير نظام الحماية المادية (1 من 3)

راجع

الكتيب 2.4

- أي قسم في تقرير نظام الحماية المادية يقوم بالتالي:
  - تعريف البنية الأساسية الحرجة الوارد وصفها بالتقرير؟
  - تحديد النقاط الرئيسية للمعلومات المستخدمة لتحديد وتعريف ووصف وترتيب أولويات مواقع البنية الأساسية الحرجة؟

Physical Protection System Report Discussion (1 of 3)	Refer To: Workbook 2.4

- Which section of the physical protection system report:
  - Identifies the critical infrastructure being described in the report?
  - Outlines the information used to locate, identify, describe, and prioritize critical infrastructure sites?

مناقشة تقرير نظام الحماية المادية (2 من 3)

راجع

الكتيب 2.4

- أي قسم في تقرير نظام الحماية المادية يقوم بالوصف التالي:
  - كيف يمكن فحص عناصر نظام الحماية المادية؟
  - ماهي التوصيات الخاصة بتحسين نظام الحماية المادية؟

Physical Protection System Report Discussion (2 of 3)	Refer To: Workbook 2.4

- Which section of the physical protection system report describes:
  - How physical protection system elements will be tested?
  - Recommendations for improving the physical protection system?

مناقشة تقرير نظام الحماية المادية (3 من 3)

راجع

الكتيب 2.4

- أي قسم في تقرير نظام الحماية المادية يقوم بالتالي:
  - احتواء نتائج تحليل التهديد؟
  - وصف الإجراءات والمداخل المستخدمة في التحليل؟

Physical Protection System Report Discussion (3 of 3)	Refer To: Workbook 2.4

- Which section of the physical protection system report:
  - Will contain the results of the threat analysis?
  - Describes the processes and approaches used in the analysis?

لحظة التعليم الإسترجاعي

- ماهي المراحل الأربع الخاصة بمنهجية تحليل نقاط الضعف؟
- ما هي المعلومات الواردة في كل قسم من أقسام تقرير نظام الحماية المادية؟

TeachBack Moment

- What are the four phases of the vulnerability analysis methodology?
- What information is included in each of the sections of the physical protection system report?

ملخص الوحدة (1 من 2)

- البنية الأساسية الحرجة
- الأمن
- تحليل نقاط الضعف
- وصف مكونات، وعناصر، ووظائف نظام الحماية المادية

Module Summary (1 of 2)

- Critical infrastructure
- Security
- Vulnerability analysis
- Components, elements, and functions of a physical protection system

ملخص الوحدة (2 من 2)

- فئات البنية الأساسية الحرجة
- أربع مراحل لمنهجية تحليل نقاط الضعف
- عناصر التقرير الخاص بنظام الحماية المادية

Module Summary (2 of 2)

- Critical infrastructure categories
- Four phases of vulnerability analysis methodology
- Elements of a physical protection system report