قاموس أمن المعلومات

مركز التميز لأمن المعلومات بجامعة الملك سعود

قاموس أمن المعلومات : لأمن المعلومات أهمية بالغة في حماية المعلومات سواء الشخصية أو الوطنية أو ما يخص قطاع الأعمال و يساهم بشكل فعال في استقرار تطوير الأنظمة واستدامتها وترسيخ ثقة المستفيدين منها. وهذه تحيّة للجهد الذي بذله أصحاب الإختصاص في مركز التميز لأمن المعلومات بجامعة الملك سعود في الاهتمام بأمن المعلومات وتشجيع التوعية وتطوير مستوى أمن المعلومات في العالم العربي حيث قاموا مشكورين بإنتاج هذا القاموس لتحقيق هدفين : أولاً: توضيح مصطلحات أمن المعلومات وشرحها لطالب العلم. ثانياً: توحيد ترجمة المصطلحات الإنجليزية الخاصة بأمن المعلومات وذلك لكي تكون المصادر العربية المتخصصة في أمن المعلومات متجانسة في ترجمة المصطلحات تيسيراً للقارئ العربي. و مع شكرنا الجزيل للأخوة الذين قاموا على إنتاج هذا القاموس قي مركز التميز لأمن المعلومات بجامعة الملك سعود وبالذات لحرصهم على توخي الدقة و استقاء المصطلحات الإنجليزية من عدة مصادر متخصصة. نشدّ على أيديهم ، و نعتبر أن هذا المشروع يستحق الإشادة والإحتفاء والتطوير ليواكب التطور والأحداث. و نحن نشكر كل من ساهم إخراج هذا المشروع للنور و نهيب بالجميع على نشر هذا القاموس وحث الكُتّاب على التقييد بترجمة المصطلحات المذكورة في القاموس عند الكتابة عن موضوعات أمن المعلومات.

Definition	تعريف المصطلح	المصطلح	Term
Ability to make use of any information system (IS) resource.	القدرة على الاستفادة من أي مورد من موارد نظام معلومات معين.	الوصول / الدخول	Access
An entity responsible for monitoring and granting access privileges for other authorized entities.	الكيان المسؤول عن مراقبة ومنح صلاحيات الوصول للجهات المُصرَّح لها.	هيئة الوصول	Access Authority
The process of granting or denying specific requests:	قبول أو رفض طلبات معينة تختص بـ		
1) for obtaining and using information and related information processing services; and	1) الحصول على (حيازة) معلومات واستخدامها و كذلك الحصول على خدمات تتعلق بمعالجتها		
2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).	2) الدخول إلى منشآت مادية محددة مثل المباني الحكومية والمؤسسات العسكرية ونقاط العبور الحدودية.	التحكم في الوصول	Access Control
A register of:	سجل يضم :		
1) users (including groups, machines, processes) who have been given permission to use a particular system resource, and	1) بيانات المستخدمين (شاملةً المجموعات والمعدات والعمليات) الممنوحين إذن باستخدام مورد نظام معين و		Access Control Lists -
2) the types of access they have been permitted.	2) أنواع الوصول المُصرَّح لهم.	قوائم التحكم في الوصول	(ACLs)
Involves	تتضمن		
1) the process of requesting, establishing, issuing, and closing user accounts;	1) عملية طلب وإنشاء وإصدار وإغلاق حسابات المستخدم		
2) tracking users and their respective access authorizations; and	2) تتبع المستخدمين وتصاريح الوصول الخاصة بهم		User Account
3) managing these functions.	3) إدارة هذه الوظائف.	إدارة حساب المستخدم	Management
The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.	الهدف الأمني الذي يولد الحاجة لتتبع أعمال جهة بعينها. يدعم ذلك عدم الإنكار ، الردع ، تشخيص الخطأ ، اكتشاف ومنع الاختراق ، القدرة على الاسترجاع بعد تنفيذ الفعل ، الإجراء القانوني.	المسؤولية	Accountability –

The official management decision given by a senior agency official to authorize operation of an system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.	قرار الإدارة الرسمية صادر من أحد الكوادر العليا لهيئة ما للتصريح بالموافقة على تشغيل نظام معلومات والقبول صراحةً بتعريض عمليات تلك الهيئة للمخاطرة (بما في ذلك رسالتها أو وظائفها أو مصداقيتها أو سمعتها) أو أصولها أو منسوبيها بناءً على تطبيق مجموعة عناصر التحكم الأمني المتفق عليها	إصدار/اعتماد الموافقة	Accreditation –
All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected.	كل ما يقوم "موظف إصدار التصريح" بالموافقة عليه من مكونات نظام معلومات باستثناء ما تم الموافقة عليه بشكل منفصل من أنظمة يتصل بها نظام المعلومات.	حدود الاعتماد	Accreditation Boundary –
The evidence provided to the authorizing official to be used in the security accreditation decision process. Evidence includes, but is not limited to:	الأدلة المقدمة إلى موظف "إصدار التصريح" لاستخدامها في عملية إصدار قرار الموافقة الأمنية. تتضمن تلك الأدلة على سبيل المثال وليس الحصر:		
1) the system security plan;	1) الخطة الأمنية للنظام		
2) the assessment results from the security certification; and	2) نتائج التقييم الصادرة عن التوثيق الأمني		
3) the plan of action and milestones.	3) خطة العمل ومراحله.	حيثيات الاعتماد	Accreditation Package –
Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.	الجهة المخول لها رسمياً سلطة أن تكون مسئولة عن تشغيل نظام معلومات معين ضمن حد مقبول من المخاطرة بعمليات هيئة معينة بما يشمل رسالتها ووظائفها ومصداقيتها وسمعتها بالإضافة إلى أصولها أو منسوبيها.	جهة الاعتماد	Accrediting Authority –
Private data, other than keys, that are required to access cryptographic modules.	هي تلك البيانات الخاصة المطلوبة للوصول إلى وحدات التشفير النمطية باستثناء المفاتيح.	بيانات التنشيط	Activation Data –
Active content refers to electronic documents that are able to automatically carry out or trigger actions on a computer platform without the intervention of a user.	يشير المحتوى النشط إلى الوثائق الالكترونية التي يمكنها تنفيذ أو تشغيل أعمال على منصة الحاسوب آلياً بدون تدخل من المستخدم.	المحتوى النشط	Active Content –
Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.	الأمن الذي يتناسب مع مدى المخاطرة والضرر الناتج من تعرض المعلومات إلى الفقد أو العبث أو الوصول غير المصرح به أو التغيير.	الأمن الكافي	Adequate Security –
Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic health information and to manage the conduct of the covered entity's workforce in relation to protecting that information.	أعمال وسياسات وإجراءات إدارية للتحكم في اختيار وتطوير وتطبيق وصيانة معايير الأمن بغرض حماية المعلومات الالكترونية وضبط تصرفات العاملين داخل الجهة المؤمَّنَة فيما يختص بحماية المعلومات.	الإجراءات الإدارية الوقائية	Administrative Safeguards –
The Advanced Encryption Standard specifies a U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. This standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits.	يحدد المعيار المتقدم للتشفير خوارزمية التشفير الصادر بشأنها موافقة من الحكومة الأمريكية التي يمكن استخدامها لحماية البيانات الالكترونية. وتمثل خوارزمية المعيار المتقدم للتشفير قالب متناظر من الترميز يمكنه تشفير وفك تشفير المعلومات. يحدد هذا المعيار خوارزمية "ريجندايل" وهي تشفير قالب متناظر يمكنها معالجة قوالب بيانات بطول 128 بت باستخدام مفاتيح ترميز طولها 128 و192 و256 بت.	المعيار المتقدم للتشفير	Advanced Encryption Standard (AES) –

A CA that acts on behalf of an Agency, and is under the operational control of an Agency.	هيئة تصديق تعمل بالنيابة عن وكالة معينة بحيث تكون خاضعة للرقابة التشغيلية لتلك الوكالة	هيئة التوثيق التابعة لوكالة	Agency Certification Authority – (CA)
A program used in distributed denial of service (DDoS) attacks that sends malicious traffic to hosts based on the instructions of a handler.	برنامج يستخدم في هجمات حجب الخدمة الموزَّعة التي ترسل سيل من البيانات الخبيثة يتدفق إلى المضيف بناءاً على تعليمات صادرة من معالج تحكم.	العميل	Agent –
The examination of acquired data for its significance and probative value to the case.	فحص بيانات مُجمِّعة نظراً لأهميتها ودلالتها للحالة موضع النقاش.	تحليل	Analysis –
A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.	برنامج يقوم بمراقبة الحاسوب أو الشبكة للتعرف على كل أنواع البرمجيات الخبيثة ومنع أو عزل ما يظهر من حالات (أعراض) تلك البرمجيات الخبيثة.	برامج مكافحة الفيروسات	Antivirus Software –
The subscriber is sometimes called an “applicant” after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.	في بعض الأحيان يطلق على المشترك اسم "مقدم الطلب" بعد تقديمه طلباً إلى هيئة التوثيق للحصول على شهادة على أن يكون ذلك قبل انتهاء إجراءات إصدار تلك الشهادة.	مُقَدِم الطلب / مشتَرِك	Applicant –
The use of information resources (information and information technology) to satisfy a specific set of user requirements.	استخدام الموارد المعلوماتية (المعلومات وتقنية المعلومات) لتلبية مجموعة محددة من متطلبات المستخدم.	تطبيق	Application –
Application content filtering is performed by a software proxy agent to remove or quarantine viruses that may be contained in email attachments, to block specific Multipurpose Internet Mail Extensions (MIME) types, or to filter other active content such as Java, JavaScript, and ActiveX® Controls.	يقوم برنامج وكيل بتصفية محتوى التطبيق لإزالة أو عزل الفيروسات التي ربما ترد في مرفقات البريد الالكتروني أو حجز أنواع معينة من امتدادات بريد الانترنت المتعددة الأغراض أو لتصفية أنواع أخرى من المحتوى النشط مثل جافا و جافاسكريبت وعناصر التحكم من نوع اكتف إكس.	تصفية محتوى التطبيق	Application Content Filtering –
Federal Information Processing Standard (FIPS) approved or National Institute of Standards and Technology (NIST) recommended. An algorithm or technique that is either	ما يتفق مع المعيار الفيدرالي لمعالجة المعلومات أو ما يصدر بشأنه توصيه من المعهد الوطني للمقاييس والتقنية بمعنى أخر خوارزمية أو طريقة		
1) specified in a FIPS or NIST Recommendation, or	1) محددة في المعيار الفيدرالي لمعالجة المعلومات أو في توصيات المعهد الوطني للمقاييس والتقنية أو		
2) adopted in a FIPS or NIST Recommendation.	2) مطبقة في المعيار الفيدرالي لمعالجة المعلومات أو توصيات المعهد الوطني للمقاييس والتقنية.	صادر بشأنه موافقة	Approved –
A mode of the cryptographic module that employs only approved security functions (not to be confused with a specific mode of an approved security function, e.g., Data Encryption Standard (DES) Cipher Block Chaining (CBC) mode).	وضعية معينة لوحدة التشفير النمطية التي تقوم بتشغيل وظائف الأمن الصادر بشأنها موافقة فقط (لا يجب الخلط بينها وبين وضعية محددة لوظيفة أمنية صادر بشأنها موافقة مثل وضعية معيار تشفير البيانات ووضعية قالب الترميز المسلسل) .	وضعية التشغيل الصادر بشأنها موافقة	Approved Mode of Operation –
A security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either	وظيفة أمنية (مثل خوارزمية التشفير أو طريقة إدارة مفتاح التشفير أو طريقة التصديق) والتي تكون إما		
a) specified in an approved standard,	أ) محددة في معيار صادر بشأنه موافقة		
b) adopted in an approved standard and specified either in an appendix of the approved standard or in a document referenced by the approved standard, or	ب) أو مُستخدَمة في معيار صادر بشأنه موافقة ومذكورة في ملحق خاص بذلك المعيار أو في وثيقة مشار إليها داخله	وظيفة أمنية صادر بشأنها موافقة	Approved Security Function –
c) specified in the list of approved security functions.	ج) أو محددة ضمن قائمة من وظائف أمنية مصدِّق عليها.		

A focused activity or action employed by an assessor for evaluating a particular attribute of a security control.	نشاط أو عمل مُركَّز يبذله المُقيِّم لقياس خاصية معينة من خواص الرقابة الأمنية.	أسلوب التقييم	Assessment Method –
A set of activities or actions employed by an assessor to determine the extent to which a security control is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	مجموعة من الأنشطة أو الأعمال يقوم بها المُقيِّم لتحديد مدى تطبيق الرقابة الأمنية بشكل صحيح وتشغيلها حسب المطلوب وتحقيقها للنتائج المرجوة منها فيما يختص باستيفاء المتطلبات الأمنية للنظام.	إجراءات التقييم	Assessment Procedure –
A major application, general support system, high impact program, physical plant, mission critical system, or a logically related group of systems.	تطبيق رئيسي أو نظام دعم عام أو برنامج له تأثير بالغ أو منشأة مادية أو نظام للتعامل مع المهام الحرجة أو مجموعة من الأنظمة المرتبطة منطقياً.	أصل / (مورد رئيسي)	Asset –
One of the five “Security Goals.” It involves support for our confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. “Adequately met” includes	أحد الأهداف الخمسة للأمن التي تتضمن دعماً لثقتنا باستيفاء الأربع أهداف الأخرى للأمن (التكامل ، استمرارية توفر الخدمة ، السرية ، المسؤولية) بشكل كافٍ من خلال طريقة محددة في التنفيذ. يتضمن الاستيفاء الكامل لتلك العناصر		
(1) functionality that performs correctly,	1) سلامة الأداء للنواحي الوظيفية		
(2) sufficient protection against unintentional errors (by users or software), and	2) ضمان حماية كافية ضد الأخطاء غير المتعمدة (من المستخدمين أو البرامج)		
(3) sufficient resistance to intentional penetration or by-pass.	3) والمقاومة الكافية لمحاولات الاختراق والتخطي المتعمدة.	تأمين / ضمان	Assurance –
Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.	مفتاحين مرتبطين أحدهما مفتاح عام والأخر خاص يتم استخدمهما لأداء عمليات متكاملة مثل التشفير وفك التشفير أو إصدار التوقيع والتحقق من صحة التوقيع.	مفاتيح غير متناظرة	Asymmetric Keys
A specific sequence of events indicative of an unauthorized access attempt.	مجموعة متسلسلة من الأحداث تشير إلى وجود محاولة وصول غير مصرح بها.	بصمة هجوم	Attack Signature –
(PKI) Policy Authority or comparable Agency body as having the authority to verify the association of attributes to an identity.	جهة تحددها هيئة السياسات الفيدرالية لسياسات البنية التحتية للمفتاح العام أو وكالة مماثلة بحيث يكون لها سلطة التحقق من توافق الخصائص مع هوية معينة.	هيئة التحقق من خصائص الهوية	Attribute Authority –
Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures	مراجعة مستقلة وفحص للسجلات والأنشطة لتقييم كفاية عناصر تحكم النظام للتأكد من موافقتها للسياسات وإجراءات التشغيل المقررة، وإصدار التوصيات حول ما هو ضروري من تغييرات في عناصر التحكم أو السياسات أو الإجراءات.	التدقيق والفحص	Audit –
Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.	سجل تاريخي لأنشطة النظام لتوفير إمكانية إعادة بناء وفحص سلسلة من الأحداث و التغييرات التي شهدها حدث معين.	بيانات التدقيق والفحص	Audit Data –

Preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. These tools generally remove records generated by specified classes of events, such as records generated by nightly backups.	معالجات تم إعدادها مسبقاً لخفض حجم سجلات الفحص والتدقيق بغرض تسهيل المراجعة اليدوية. قبل إجراء المراجعة الأمنية تستطيع هذه الأدوات إزالة العديد من سجلات التدقيق والفحص المعروفة بانخفاض أهميتها الأمنية. تقوم هذه الأدوات عموماً بإزالة أنواع محددة من الأحداث مثل تلك السجلات الناتجة عن عمليات النسخ الاحتياطي الدورية التي تحدث في نهاية كل ليلة.	أدوات تيسير التدقيق والفحص	Audit Reduction Tools –
A record showing who has accessed an Information Technology (IT) system and what operations the user has performed during a given period.	سجل يوضح من قام بالدخول إلى نظام تقنية معلومات و العمليات التي قام بتنفيذها أثناء فترة معينة.	سجل الفحص و المراجعة	Audit Trail –
To confirm the identity of an entity when that identity is presented.	التأكد من هوية جهة معينة عند تقديم تلك الهوية.	يصدِّق على / يتحقق من هوية	Authenticate –
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. The process of establishing confidence of authenticity. Encompasses identity verification, message origin authentication, and message content authentication. A process that establishes the origin of information or determines an entity's identity.	التأكد من صحة هوية الخاصة بأحد المستخدمين أو العمليات أو الأجهزة. يكون ذلك عادة كأحد متطلبات السماح بالوصول إلى الموارد الموجودة في نظام معلومات معين. عملية تأسيس الثقة وتشمل التحقق من صحة الهوية والتحقق من مصدر الرسالة ومحتواها. عملية تهدف إلى تحديد مصدر المعلومات أو هوية جهة ما.	التصديق / التحقق من الهوية	Authentication –
A cryptographic checksum based on an approved security function (also known as a Message Authentication Code (MAC)).	معادلة تشفير حسابية تعتمد على وظيفة أمنية صادر بشأنها موافقة (تعرف أيضاً باسم شفرة رسالة التصديق) .	شفرة التحقق من الهوية	Authentication Code –
The process of establishing confidence in user identities electronically presented to an information system.	عملية إثبات الثقة في هويات المستخدمين التي تقدم الكترونياً لنظام معلومات.	التحقق من الهوية الكترونياً	Electronic Authentication –
Hardware or software-based mechanisms that force users to prove their identity before accessing data on a device.	آليات تعتمد على الأجهزة أو البرامج بحيث تُجبِر المستخدمين على إثبات هوياتهم قبل الوصول للبيانات الموجودة على أحد الأجهزة.	آلية التحقق من الهوية	Authentication Mechanism –
A block cipher mode of operation that can provide assurance of the authenticity and, therefore, the integrity of data.	وضعية تشغيل تستخدم قالب ترميز معين يمكنها تأمين الثقة في هوية المستخدم وبالتالي في تكامل البيانات.	وضعية التحقق من الهوية	Authentication Mode –
A well specified message exchange process that verifies possession of a token to remotely authenticate a claimant. Some authentication protocols also generate cryptographic keys that are used to protect an entire session, so that the data transferred in the session is cryptographically protected.	امتلاك احد الرموز المميزة بغرض التحقق عن بعد من هوية الشخص الذي يطلب التعامل مع نظام معين. بعض برتوكولات التصديق تقوم بإنشاء مفاتيح تشفير تُستخدَم لتوفير الحماية طوال فترة التعامل مع النظام ولذلك تكون البيانات المنقولة خلال تلك الفترة محمية بفضل تشفيرها.	برتوكول التحقق من الهوية	Authentication Protocol –
A pair of bit strings associated to data to provide assurance of its authenticity.	زوجين من السلاسل النصية مرتبطة بالبيانات للتأكد من مصداقيتها.	علامة التصديق	Authentication Tag –
Authentication information conveyed during an authentication exchange.	معلومات التحقق المتبادلة أثناء التحقق من صحة الهوية	الرمز المميز للتحقق من الهوية	Authentication Token –
The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.	خاصية أن تكون أصلياً وقابل للتحقق من هويتك والوثوق بها من خلال منح الثقة في صحة الإرسال والرسالة ومرسلها.	خاصية المصداقية	Authenticity –

The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.	قرار الإدارة الرسمية الصادر من أحد الكوادر العليا لهيئة ما لاعتماد الموافقة على تشغيل نظام معلومات والقبول علانيةً بتعريض عمليات تلك الهيئة للمخاطرة (بما في ذلك رسالتها ووظائفها ومصداقيتها وسمعتها) أو أصولها أو منسوبيها بناءاً على تنفيذ مجموعة من عناصر التحكم الأمني المتفق عليها.	تصريح	Authorization –
Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Accreditation Authority.	الموظف (الكيان) المسئول رسمياً عن تشغيل نظام معلومات معين ضمن حد مقبول من المخاطرة بعمليات هيئة معينة (بما يشمل رسالتها ووظائفها ومصداقيتها وسمعتها) بالإضافة إلى أصولها أو منسوبيها.	موظف إصدار التصريح	Authorizing Official –
Individual selected by an authorizing official to act on their behalf in coordinating and carrying out the necessary activities required during the security certification and accreditation of an information system.	شخص يختاره موظف إصدار التصريح للعمل نيابة عنه في تنسيق وتنفيذ الأنشطة الضرورية المطلوبة أثناء التوثيق و الاعتماد الأمني لأحد أنظمة المعلومات.	مندوب إصدار التصريح	Authorizing Official – Designated Representative –
The transport of cryptographic keys, usually in encrypted form, using electronic means such as a computer network (e.g., key transport/agreement protocols).	نقل مفاتيح التشفير (عادة بطريقة مشفرة) باستخدام وسائل الكترونية مثل شبكات الحاسوب كما هو الحال في بروتوكولات نقل مفتاح التشفير وقبوله.	النقل الآلي للمفتاح	Automated Key Transport –
An algorithm which creates random passwords that have no association with a particular user.	خوارزمية تقوم بإنشاء كلمات مرور العشوائية غير مرتبطة بمستخدم معين.	مولد كلمة المرور الآلي	Automated Password Generator –
Ensuring timely and reliable access to and use of information.	التأكد من إمكانية الوصول إلى المعلومات واستخدامها في الوقت المناسب وبشكل يُعتمَد عليه.	استمرارية توفر الخدمة	Availability –
Activities which seek to focus an individual's attention on an (information security) issue or set of issues.	الأنشطة التي تسعى لجذب انتباه الأفراد إلى موضوع أو مجموعة من الموضوعات في أمن المعلومات.	الوعي بأمن المعلومات	Information Security Awareness –
A copy of files and programs made to facilitate recovery if necessary.	نسخة من الملفات والبرامج لتسهيل عملية الاسترجاع في حالة الضرورة.	نسخة احتياطية	Backup –
The minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity and/or availability protection.	الحد الأدنى من عناصر التحكم الأمنية المطلوبة لحماية نظام معلومات معين بناءاً على الاحتياجات المحددة لحماية سرية وتكامل و/أو استمرارية توفر خدمة هذا النظام.	الحد الأدنى من الأمن	Baseline Security –
Monitoring resources to determine typical utilization patterns so that significant deviations can be detected.	مراقبة الموارد لتحديد نماذج الاستخدام الأمثل بهدف كشف الانحرافات الخطيرة.	الرقابة والمتابعة والضبط	Baselining –
A bastion host is typically a firewall implemented on top of an operating system that has been specially configured and hardened to be resistant to attack.	هو جدار حماية نموذجي يجرى تنصيبه على نظام تشغيل جرى إعداده وتقويته خصيصاً ليكون مقاوم للهجمات.	جهاز المضيف المحصن	Bastion Host –
What an individual who has completed the specific training module is expected to be able to accomplish in terms of IT security-related job performance.	ما يتوقع من شخص تلقى تدريباً خاصاً يمّكنه من إظهار مردود ما تعلمه عن أمن المعلومات من خلال أداءه الوظيفي.	المحصلة السلوكية	Behavioral Outcome –

Process of associating two related elements of information. An acknowledgement by a trusted third party that associates an entity's identity with its public key. This may take place through	عملية ضم عنصرين مرتبطين من عناصر المعلومات. اعتراف من طرف ثالث موثوق يقوم بربط هوية جهة معينة بمفتاح التشفير العام لتلك الجهة. يمكن أن يتم تطبيق ذلك من خلال		
(1) a certification authority's generation of a public key certificate,	1) قيام هيئة توثيق بإصدار شهادة مفتاح التشفير العام		
(2) a security officer's verification of an entity's credentials and placement of the entity's public key and identifier in a secure database, or	2) قيام موظف أمن بالتحقق من بيانات دخول تلك الجهة ووضع مفتاح التشفير العام لتلك الجهة مع رقم مميز في قاعدة بيانات آمنة أو		
(3) an analogous method.	3) إتباع الأسلوب التناظري.	الربط	Binding –
A physical or behavioral characteristic of a human being. A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and handwriting samples are all examples of biometrics.	ميزة جسدية أو سلوكية من مميزات الإنسان. ميزة جسدية أو صفة سلوك الشخصي قابلة للقياس تُستخدَم في تعريف شخصية مقدم الطلب أو التحقق منها. تعد صور الوجه وبصمات الأصابع ونماذج الكتابة من أمثلة القياسات الحيوية.	قياس حيوي	Biometric –
The stored electronic information pertaining to a biometric. This information can be in terms of raw or compressed pixels or in terms of some characteristic (e.g. patterns.)	هي تلك المعلومات الالكترونية المخزنة بخصوص مقياس حيوي معين و تكون في شكل نقاط خام أو مضغوطة أو في شكل له بعض الخصائص مثل النماذج.	معلومات القياس الحيوي	Biometric Information –
An automated system capable of:	نظام آلي قادر على:		
1) capturing a biometric sample from an end user;	1) الحصول على عينة قياس حيوية من المستخدم النهائي		
2) extracting biometric data from that sample;	2) استخلاص بيانات القياس الحيوي من تلك العينة		
3) comparing the biometric data with that contained in one or more reference templates;	3) مقارنة بيانات القياس الحيوي بتلك الموجودة في نموذج أو أكثر		
4) deciding how well they match; and	4) تقدير مدى التماثل بينهما و		
5) indicating whether or not an identification or verification of identity has been achieved.	5) الإشارة إلى ما إذا كان التعرف أو التحقق من صحة الشخصية قد تم إنجازه أم لا.	نظام قياس حيوي	Biometric System –
A characteristic of biometric information (e.g. minutiae or patterns.)	أحد خواص معلومات القياس الحيوي (تفاصيل أو شكل مثلاً) .	نموذج قياس حيوي	Biometric Template –
Malicious code that uses multiple methods to spread.	شفرة برمجية خبيثة تستخدم عدة أساليب كي تدعم انتشاره.	الهجوم المختَلَط	Blended Attack –
Sequence of binary bits that comprise the input, output, State, and Round Key. The length of a sequence is the number of bits it contains. Blocks are also interpreted as arrays of bytes.	والحالة والمفاتيح المتعاقبة. طول ذلك التسلسل هو عدد وحدات البت التي يتضمنها. تُفسر القوالب أيضاً على أنها مصفوفة من وحدات البايت.	قالب	Block –
A symmetric key cryptographic algorithm that transforms a block of information at a time using a cryptographic key. For a block cipher algorithm, the length of the input block is the same as the length of the output block.	خوارزمية تشفير متناظرة تُحوِّل قالب من المعلومات في وقت واحد مستخدمة مفتاح تشفير. من صفات تلك الخوارزمية أن طول قالب المدخلات هو نفس طول قالب المخرجات.	تشفير القالب	Block Cipher –
A family of functions and their inverses that is parameterized by a cryptographic key; the function maps bit strings of a fixed length to bit strings of the same length.	باستخدام مفتاح تشفير حيث تقوم الدالة بتحويل سلسلة ذات طول محدد من وحدات البت إلى سلسلة من وحدات البت لها نفس الطول.	خوارزمية تشفير القالب	Block Cipher Algorithm –

A virus that plants itself in a system's boot sector and infects the master boot record.	فيروس يقوم بزراعة نفسه داخل قطاع تشغيل نظام معين ثم يصيب سجل التشغيل الرئيسي.	فيروس قطاع التشغيل	Boot Sector Virus –
Monitoring and control of communications at the external boundary between information systems completely under the management and control of the organization and information systems not completely under the management and control of the organization, and at key internal boundaries between information systems completely under the management and control of the organization, to prevent and detect malicious and other unauthorized communication, employing controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels).	فرض الرقابة والتحكم في الاتصالات على الحدود الخارجية بين أنظمة المعلومات الخاضعة بالكامل لإدارة ورقابة منظمة معينة وتلك الأنظمة التي لا تخضع لإدارتها ورقابتها بشكل كامل، بالإضافة إلى فرضهما على الحدود الداخلية الرئيسية بين نظم المعلومات التي تخضع بأكملها لإدارة ورقابة تلك المنظمة بغرض منع واكتشاف محاولات الاتصال الخبيثة وغير المصرح بها وكذلك استعمال وسائل اتصال يمكن التحكم بها مثل الوكيل وبوابات الوصول والموجهات وجدران الحماية والقنوات المشفرة.	حماية حدود النظام	Boundary Protection –
A boundary router is located at the organizations boundary to an external network.	موجه خارجي يوضع على نقاط اتصال المنظمات مع شبكة خارجية.	موجه اتصال خارجي	Boundary Router –
A method of accessing an obstructed device through attempting multiple combinations of numeric and/or alphanumeric passwords.	أسلوب لمحاولة الدخول على أحد الأجهزة التي تمثل عائقاً من خلال إجراء المحاولات باستخدام كلمات مرور متنوعة تجمع عدد من الحروف و/أو الأرقام.	طريقة الاستقصاء في الهجوم على كلمة المرور	Brute Force Password Attack –
A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system.	شرط في قناة الاتصال يمكن من خلاله وضع عدد اكبر من المدخلات في منطقة مخصصة لاحتجاز البيانات بما يفوق قدرتها الاستيعابية لذلك من خلال استبدال المعلومات الموجودة بالكتابة عليها. يستخدم المهاجمون ذلك الشرط لإسقاط النظام أو إدخال شفرات خاصة تم إعدادها بمهارة عالية تسمح لهم بالسيطرة على النظام والتحكم فيه.	إغراق ذاكرة التخزين المؤقت	Buffer Overflow –
A method of overloading a predefined amount of space in a buffer, which can potentially overwrite and corrupt data in memory.	أسلوب التحميل الزائد للبيانات داخل مساحة محددة سلفاً في منطقة حفظ البيانات مما يؤدى إلى احتمالية الكتابة على الكتابة الموجودة في الذاكرة أو تخريبها.	الهجوم بإغراق ذاكرة التخزين المؤقت	Buffer Overflow Attack –
The documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption.	توثيق مجموعة من التعليمات والإجراءات المُعَدَّة سلفاً لوصف كيفية الحفاظ على وظائف العمل داخل منظمة معينة أثناء وبعد حدوث خلل خطير.	خطة الحفاظ على استمرارية العمل	Business Continuity Plan (BCP) –
An analysis of an information technology (IT) system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.	تحليل لما يخص نظام تقنية المعلومات من متطلبات وعمليات وعلاقات متبادلة تُستخدَم في توصيف ما يخص النظام من متطلبات طارئة وأولويات في حالة حدوث خلل خطير.	تحليل متطلبات الطوارئ	Business Impact Analysis (BIA) –
The documentation of a predetermined set of instructions or procedures that describe how business processes will be restored after a significant disruption has occurred.	توثيق لمجموعة من التعليمات والإجراءات المحددة سلفاً تصف كيفية استعادة حركة العمل بعد حدوث خلل خطير.	خطة استعادة حركة العمل	Business Recovery-Resumption Plan – (BRP)
The method of taking a biometric sample from an end user.	أسلوب الحصول على عينة قياس حيوي من مستخدم نهائي.	التقاط	Capture –
An individual possessing an issued Personal Identity Verification (PIV) card.	شخص معين يمتلك بطاقة شخصية لتحديد الهوية.	حامل البطاقة	Cardholder –
A digital representation of information which at least	شكل رقمي للبيانات يوفر على الأقل ما يلي		

1) identifies the certification authority issuing it, 2) names or identifies its subscriber, 3) contains the subscriber's public key, 4) identifies its operational period, and 5) is digitally signed by the certification authority issuing it. A set of data that uniquely identifies an entity, contains the entity's public key and possibly other information, and is digitally signed by a trusted party, thereby binding the public key to the entity. Additional information in the certificate could specify how the key is used and its cryptoperiod.	1) تحديد هيئة التوثيق التي أصدرت الشهادة 2) أسماء المشتركين فيها 3) المفتاح العام للمشترك 4) يحدد الفترة التي تكون خلالها تلك الشهادة صالحة للعمل مجموعة من البيانات التي تشير بشكل منفرد إلى كيان واحد بحيث تحتوى على المفتاح العام لذلك الكيان وأي معلومات أخرى ممكنة. تكون الرسالة مُصَدق عليها رقمياً من طرف ثالث موثوق به وعليه يتم ربط المفتاح العام بذلك الكيان. هناك معلومات إضافية في الشهادة الرقمية يمكن من خلالها تحديد كيفية استخدام المفتاح ومدة تشفيره.	شهادة رقمية	Certificate –
A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.	شكل خاص من السياسات الإدارية يتواءم مع معاملات إلكترونية تُطبق أثناء إدارة الشهادة الرقمية. تعالج سياسة الشهادة الرقمية كل النواحى المرتبطة باصدارها واستخراجها وتوزيعها وحساباتها واستعادتها وكذلك إدارتها. وبشكل غير مباشر يمكن لسياسة الشهادة الرقمية أن تتحكم فى المعاملات المُنجزة بنظام اتصالات تتوفر له الحماية من خلال نظام أمن يعتمد على الشهادة الرقمية. من خلال التحكم في الامتدادات الخاصة بالشهادات الرقمية الحرجة يمكن لتلك السياسات وما يصاحبها من تقنية المتابعة والضبط دعم تدابير الخدمات الأمنية التي تطلبها تطبيقات معينة.	سياسة الشهادة الرقمية	Certificate Policy (CP) –
A Certification Authority (CA) or a Registration Authority (RA).	هيئة توثيق أو هيئة تسجيل.	هيئة إدارة الشهادات الرقمية	Certificate Management Authority (CMA) –
Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a Certification Authority (CA) managing certificates.	معلومات غير مضافة للشهادة الرقمية مثل العنوان البريدي للمشترك. ربما تستخدم هيئة توثيق معين تلك البيانات لإدارة الشهادات الرقمية.	معلومات مرتبطة بالشهادات الرقمية	Certificate-Related Information –
A list of revoked public key certificates created and digitally signed by a Certification Authority.	قائمة شهادات المفتاح العام الملغية. يتم إصدار تلك القائمة والتوقيع عليها رقمياً بواسطة هيئة توثيق.	قائمة الشهادات الرقمية الملغاة	Certificate Revocation List (CRL) –
A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.	كيان موثوق فيه توفر بشكل مباشر لطرف تابع امكانية التحقق من مصداقية شهادة رقمية معينة وربما أيضاً يوفر معلومات إضافية عن الشهادة الخاضعة للفحص .	هيئة تحديد حالة الشهادة الرقمية	Certificate Status Authority –
A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	تقييم شامل لكل عناصر التحكم والرقابة الإدارية والتشغيلية والفنية داخل نظام معلومات دعماً للحصول على الموافقة الأمنية بغرض تحديد مدى تُطبيق عناصر التحكم تطبيقاً سليماً ومدى عملها طبقاً للطريقة المقصودة وتحقيقها للنتائج المرجوة لتلبية متطلبات أمن النظام	توثيق	Certification –

The individual, group, or organization responsible for conducting a security certification.	الفرد أو المجموعة أو المنظمة المسؤولة عن إدارة التوثيق الأمني.	وكيل التوثيق الأمني	Certification Agent –
A trusted entity that issues and revokes public key certificates. The entity in a public key infrastructure (PKI) that is responsible for issuing certificates and exacting compliance to a PKI policy.	كيان موثوق يقوم بإصدار وإلغاء شهادات المفتاح العام. ذلك الكيان الموجودة في البنية التحتية للمفتاح العام حيث يتولى مسئولية إصدار الشهادات والتأكد من الالتزام بسياسة البنية التحتية للمفتاح العام.	هيئة التوثيق	Certification Authority (CA) –
The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.	مجموعة الأجهزة والموظفين والإجراءات والمباني التي تستخدمها هيئة التوثيق لإصدار شهادة التوثيق وإلغاءها.	مرفق هيئة التوثيق	Certification Authority Facility –
A statement of the practices that a Certification Authority employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this Certificate Policy, or requirements specified in a contract for services).	إعلان بالممارسات التي تتخذها هيئة التوثيق في سبيل إصدار أو وقف أو إلغاء أو تجديد الشهادات بالإضافة إلى توفير إمكانية الوصول إليها في ظل متطلبات معينة كتلك المحددة في سياسة الشهادة أو عقد توفير الخدمات.	بيان بممارسة أعمال التوثيق	Certification Practice Statement (CPS) –
A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.	عملية تتبع حركة الدليل من خلال جمعه وحمايته وتحليل دورة تطوره بواسطة توثيق كل شخص تناوله بالتغيير وكذلك تاريخ ووقت تجميعه أو نقله والغرض من ذلك النقل.	سلسلة متابعة الدليل	Chain of Custody –
An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a shared secret (often by hashing the challenge and secret together) to generate a response that is sent to the verifier. The verifier knows the shared secret and can independently compute the response and compare it with the response generated by the claimant. If the two are the same, the claimant is considered to have successfully authenticated himself. When the shared secret is a cryptographic key, such protocols are generally secure against eavesdroppers. When the shared secret is a password, an eavesdropper does not directly intercept the password itself, but the eavesdropper may be able to find the password with an off-line password guessing attack	بروتوكول تصديق يقوم فيه المسؤول عن التحقق من الهوية بإرسال سؤال إلى صاحب الطلب الذي يقوم بدوره بدمج ذلك السؤال مع سر مشترك (عادة يتم دمج السؤال والسر معاً) لتوليد إجابة تُرسَل إلى المسؤول عن التحقق حيث يكون لديه علم بإجابة السؤال المشترك ويمكنه معرفتها بشكل مستقل ومقارنتها بالإجابة التي تلقاها من صاحب الطلب. إذا تطابقت الإجابتين يعتبر صاحب الطلب قد نجح فى الحصول على تصديق لهويته. عندما يكون السؤال المشترك عبارة عن مفتاح تشفير فإن مثل هذه البرتوكولات عموماً تتسم بالأمان ضد محاولات التصنت. أما إذا كان السؤال المشترك "كلمة مرور" فان المتصنت لا يتعرض لكلمة السر مباشرة ولكنه ربما يستطيع الحصول عليها من خلال شن هجوم لتخمين كلمة السر دون الاتصال بالشبكة.	بروتوكول سؤال وإجابة تحديد الهوية	Challenge-Response Protocol –
Agency official responsible for:	موظف الوكالة المسؤول عن:		

1) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, executive orders, directives, policies, regulations, and priorities established by the head of the agency;	1) إسداء النصيحة ومد يد العون لرئيس الوكالة التنفيذي والآخرين من كوادر الإدارة العليا للتأكد من تحصيل تقنية المعلومات وترتيب موارد البيانات بشكل يتوافق مع القوانين والأوامر التنفيذية والتعليمات والسياسات واللوائح والأولويات التي أرساها رئيس الوكالة.		
2) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.	2) إعداد وصيانة وتسهيل تطبيق بنية معلوماتية سليمة تتسم بالتكامل داخل الوكالة		
	3) إنشاء تصميم فَعَّال وطريقة تشغيل متقنة لكل موارد المعلومات الرئيسية بما في ذلك تحسين إجراءات العمل داخل الوكالة.	رئيس قطاع المعلومات	Chief Information Officer (CIO) –
Series of transformations that converts plaintext to ciphertext using the Cipher Key.	سلسلة من التحويلات التي تحول نص غير مُشفَّر إلى نص مُشَفَر باستخدام مفتاح ترميز.	عملية الترميز	Cipher –
A secret-key block-cipher algorithm used to encrypt data and to generate a Message Authentication Code (MAC) to provide assurance that the payload and the associated data are authentic.	خوارزمية قالب تشفير ذات مفتاح سرى تُستخدَم في تشفير البيانات واستخراج شفرة التصديق الخاصة بالرسالة بغرض التأكد من موثوقية الرسالة ومحتوياتها من بيانات.	قالب الترميز المسلسل-شفرة التصديق الخاصة بالرسالة	Cipher Block Chaining-Message Authentication Code (CBC-MAC) –
Secret, cryptographic key that is used by the Key Expansion routine to generate a set of Round Keys; can be pictured as a rectangular array of bytes, having four rows and Nk columns.	مفتاح تشفير سرى تستخدمه دالة تمديد المفتاح لتوليد مجموعة من المفاتيح المتعاقبة ويمكن تصويرها كمصفوفة مستطيلة من وحدات البايت تتألف من أربعة صفوف وعدد غير محدد من الأعمدة.	مفتاح الترميز	Cipher Key –
Negotiated algorithm identifiers. Cipher suites are identified in human readable form using a pneumonic code.	مجموعة من عناصر التعريف تتسم بقابلية خوارزميتها للنقاش. يجري تعريف حزم الترميز بطريقة مقروءة بشرياً باستخدام شفرة مخزنة يمكن تذكرها.	حزمة الترميز	Cipher Suite –
Data output from the Cipher or input to the Inverse Cipher.	مخرجات البيانات من عملية الترميز أو مدخلاتها في عملية الترميز المعكوس.	نص الترميز	Ciphertext –
A party whose identity is to be verified using an authentication protocol. An entity which is or represents a principal for the purposes of authentication, together with the functions involved in an authentication exchange on behalf of that entity. A claimant acting on behalf of a principal must include the functions necessary for engaging in an authentication exchange. (e.g., a smartcard (claimant) can act on behalf of a human user (principal))	الطرف الذي يُتحقَق من هويته باستخدام بروتوكول التصديق. كيان يكون هو نفسه رئيساً أو ممثلاً عن رئيس لاستيفاء أغراض التحقق من الهوية بالإضافة إلى الوظائف التي تتطلب تبادل لبيانات التصديق. المدعى الذي يؤدى العمل نيابة عن الرئيس يجب أن يتحلى بالصلاحيات اللازمة للشروع في تبادل بيانات التصديق على سبيل المثال امتلاك البطاقات الذكية الخاصة بالمدعى يمكن أن ينوب عن العنصر البشرى وهو الرئيس في تلك الحالة.	مقدم الطلب / المدعى	Claimant –

Information that has been determined pursuant to Executive Order (E.O.) 13292 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.	معلومات تم تصنيفها بناءاً على القرار التنفيذي رقم 13292 أو أي قرارات تالية بغرض الحماية ضد الكشف غير المصرح به ويتم تميزها للإشارة إلى سريتها عند تحويلها إلى الأرشيف كملفات وثائقية.	معلومات سرية / مصنفة	Classified Information –
A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.	أحد مكونات نظام معين عادة ما تكون عملية حاسوبية تعمل نيابة عن أحد العناصر البشرية حيث تستفيد من أحد الخدمات التي يوفرها خادم معين.	العميل (برنامج/تطبيق)	Client (Application) –
A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site.	منشأة احتياطية تضم ما يلزم من تجهيزات كهربية ومادية لتكون منشأة للحاسوب ولكنها لا تحتوى على أجهزة الحاسوب. يكون الموقع على استعداد لاستقبال أجهزة الحاسوب البديلة في حال وجوب انتقال المستخدمين من مبنى الحاسوب الرئيسي إلى مبنى آخر بديل.	موقع بارد	Cold Site –
Two or more distinct inputs produce the same output.	اثنين أو أكثر من عناصر المدخلات تنتج نفس المخرجات.	تعارض/تصادم	Collision –
Security control that can be applied to one or more agency information systems and has the following properties:	الرقابة الأمنية التي يمكن تطبيقها على واحد أو أكثر من أنظمة معلومات وكالة حيث تتسم بالخصائص التالية:	الرقابة الأمنية المشتركة	Common Security Control –
1) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and	1) من الممكن إسناد تطوير وتنفيذ وتقييم الرقابة إلى موظف مسؤول أو أحد عناصر المنظمة (غير مالك نظام المعلومات) و		
2) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.	2) يمكن استخدام نتائج تقييم الرقابة لدعم التوثيق الأمني واعتماد الموافقة على العمليات الخاصة بنظام معلومات الوكالة التي تم تطبيق الرقابة فيها.		
A dictionary of common names for publicly known IT system vulnerabilities.	قاموس يضم الأسماء الشائعة لأشهر الثغرات في أنظمة المعلومات.	الثغرات والمخاطر الأمنية الشائعة	Common Vulnerabilities and Exposures (CVE) –
The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high security control baselines, that provide equivalent or comparable protection for an information system.	عناصر التحكم الإدارية والتشغيلية والفنية مثل إجراءات الوقاية وعوامل المقاومة التي يتم العمل بها داخل منظمة بدلاً من عناصر التحكم الموصى بها في الحد الأدنى من عناصر التحكم الأمني المنخفض أو المتوسط أو المرتفع بغرض توفير درجة مساوية أو مكافئة من الحماية لنظام معلومات معين.	عناصر التحكم المكافئة	Compensating Controls –
The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system.	عناصر التحكم الإدارية والتشغيلية والفنية مثل إجراءات الوقاية وعوامل المقاومة التي يتم العمل بها داخل منظمة بدلاً من عناصر التحكم الموصى بها في الحد الأدنى من عناصر التحكم الأمني المنخفض أو المتوسط أو المرتفع المذكورة في المنشور الخاص رقم 880-53 الصادر من المعهد الوطني للمقاييس والتقنية في أمريكا بغرض توفير درجة مساوية أو مكافئة من الحماية لنظام معلومات.	عناصر التحكم الأمني المكافئة	Compensating Security Controls –

Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. The unauthorized disclosure, modification, substitution or use of sensitive data (including plaintext cryptographic keys and other critical security parameters).	الإفصاح عن معلومات لأشخاص غير مصرح لهم أو انتهاك السياسة الأمنية لنظام بالإفصاح عن أو تغيير أو تخريب أو فقد شيء سواء بنية مبيتة أو عن غير قصد. الإفصاح عن بيانات حساسة أو تغيير ها أو تبديلها أو استخدامها بدون تصريح (بما في ذلك مفاتيح تشفير النصوص غير المُشفَّرة وغيرها من المعايير الأمنية الحرجة.	انتهاك أمنى	Compromise –
The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.	جمع بيانات متعلقة بالحاسوب والاحتفاظ بها وتحليلها من أجل أغراض تقصى الحقائق بطريقة تحافظ على تكامل البيانات.	التحليل الجنائي لبيانات الحاسوب	Computer Forensics –
A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.	انتهاك أو تهديد خطير بانتهاك السياسات الأمنية للحاسوب أو سياسات الاستخدام المتفق عليها أو الممارسات القياسية لأمن الحاسوب.	حادثة أمن الحاسوب	Computer Security Incident –
A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability).	قوة مهيئة للمساعدة فى الاستجابة للحوادث المرتبطة بأمن الحاسوب. يطلق عليها أيضاً فريق الاستجابة لحوادث الحاسوب أو مركز الاستجابة لحوادث الحاسوب أو قوة الاستجابة لحوادث الحاسوب	فريق التعامل مع الحوادث الأمنية للحاسوب	Computer Security Incident Response Team (CSIRT) –
A resource, tool, or mechanism used to maintain a condition of security in a computerized environment. These objects are defined in terms of attributes they possess, operations they perform or are performed on them, and their relationship with other objects.	مورد أو أداة أو آلية تُستَخدم للحفاظ على حالة من الأمن في بيئة تقوم على الحاسوب. توصف هذه العناصر طبقاً للخواص التي تمتلكها والعمليات التي تُنَفذها أو ما يتم تنفيذه عليها من عمليات بالإضافة إلى علاقاتها بالعناصر الأخرى.	عنصر أمن الحاسوب	Computer Security Object (CSO) –
A collection of Computer Security Object names and definitions kept by a registration authority.	مجموعة من أسماء وتعريفات عناصر أمن الحاسوب محفوظة بواسطة هيئة للتسجيل.	سجل عناصر أمن الحاسوب	Computer Security Objects Register –
A computer virus is similar to a Trojan horse because it is a program that contains hidden code, which usually performs some unwanted function as a side effect. The main difference between a virus and a Trojan horse is that the hidden code in a computer virus can only replicate by attaching a copy of itself to other programs and may also include an additional "payload" that triggers when specific conditions are met.	يشبه فيروس الحاسوب حصان طروادة لأنه برنامج يحتوى على شفرة مخفية يقوم عادة بتنفيذ بعض الوظائف غير المرغوبة. الاختلاف الرئيسي بين الفيروس وحصان طروادة هو أن الشفرة المخفية داخل فيروس الحاسوب يستطيع التكاثر من خلال إلصاق نسخة منه ببرامج أخرى وربما تحتوى أيضاً على عوامل تخريب تعمل فقط إذا توفرت شروط معينة.	فيروس الحاسوب	Computer Virus –
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	الاحتفاظ بقيود مصرح بها على الوصول إلى المعلومات و الإفصاح عنها بما في ذلك وسائل حماية معلومات الخصوصية و الملكية الشخصية. خاصية أن تظل البيانات الحساسة غير معلن عنها للذين لم يُصرَح لهم من الأفراد أو الكيانات أو العمليات.	مبدأ السرية والخصوصية	Confidentiality –
Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.	عملية للتحكم في إجراء التغييرات للأجهزة والبرمجيات وبرامج التشغيل المثبتة في ذاكرة القراءة والوثائق للتأكد من حماية نظام المعلومات ضد التغييرات الخاطئة قبل أو أثناء أو بعد تطبيق النظام.	التحكم في تهيئة/إعدادات النظام	Configuration Control –

Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.	ما تم تخطيطه من سياسة وإجراءات إدارية لحفظ واسترجاع عمليات التشغيل بما فيها عمليات الحاسوب على الأرجح في مكان بديل وذلك لاستخدامه في حالات الطوارئ وسقوط النظام والكوارث.	خطة الطوارئ	Contingency Plan –
A predetermined set of instructions or procedures that describe how an organization’s essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations.	مجموعة من التعليمات والإجراءات المحددة سلفاً تُبين كيفية استمرار تشغيل الوظائف الأساسية لمنظمة معينة لمدة 30 يوم نتيجة لحدوث كارثة وذلك قبل العودة إلى الطريقة المعتادة في تشغيل العمليات.	خطة استمرار التشغيل	Continuity of Operations Plan (COOP) –
The documentation of a predetermined set of instructions or procedures mandated by Office of Management and Budget (OMB) A-130 that describe how to sustain major applications and general support systems in the event of a significant disruption.	توثيق لمجموعة من التعليمات والإجراءات المحددة سلفاً فرضها رسمياً مكتب الإدارة والميزانية A-130 حيث تبين كيفية استمرار عمل التطبيقات الرئيسية وأنظمة الدعم العام في حال حدوث خلل خطير.	خطة استمرار الدعم	Continuity of Support Plan –
Information that is entered into a cryptographic module for the purposes of directing the operation of the module.	المعلومات المُدخلة إلى وحدة تشفير نمطية بغرض إدارة تشغيل الوحدة.	معلومات التحكم	Control Information –
Mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system).	آلية تُيسر الحكم على سياسات أمنية لأنظمة مترابطة مختلفة (مثل التحكم في تدفق المعلومات من و إلى نظام مرتبط بغيره)	التحكم في الربط بين السياسات الأمنية	Controlled Interface –
A piece of information supplied by a web server to a browser, along with requested resource, for the browser to store temporarily and return to the server on any subsequent visits or requests.	معلومة يُرسلها خادم الويب إلى برنامج المتصفح مرفقة بالمورد المطلوب. يقوم المتصفح بتخزين تلك المعلومة مؤقتاً على أن يعيدها لخادم الويب مرة أخرى في الزيارات أو الطلبات التالية.	ملفات جمع البيانات	Cookie –
A mode of operation for a symmetric key block cipher algorithm. It combines the techniques of the Counter (CTR) mode and the Cipher Block Chaining-Message Authentication Code (CBC-MAC) algorithm to provide assurance of the confidentiality and the authenticity of computer data.	وضعية تشغيل لخوارزمية تشفير قالب بمفتاح متناظر. وهي تجمع بين أساليب وضعية العداد و خوارزمية "مسلسل قالب التشفير / شفرة التصديق الخاصة بالرسالة" للتأكيد على سرية و مصداقية بيانات الحاسوب	أسلوب العداد	Counter with Cipher Block Chaining-Message Authentication Code (CCM) –
Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.	أعمال أو أدوات أو إجراءات أو أساليب أو معايير أخرى تعمل على تقليل الثغرات الأمنية في نظام المعلومات. تعتبر مرادفاً لعناصر التحكم الأمني وإجراءات الوقاية.	عوامل المقاومة	Countermeasures –
An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person. Evidence attesting to one’s right to credit or authority.	عنصر يعمل على الربط رسمياً بين الهوية (وبشكل اختياري بعض الخواص الإضافية) وبين رمز مميز يمتلكه ويتحكم فيه شخص معين. أدلة تؤيد مصداقية أو صلاحية شخص معين.	عناصر اعتماد المصداقية	Credential –
A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The CSP may encompass Registration Authorities and verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use.	كيان موثوق يقوم بإصدار أو تسجيل الرموز المميزة للمشتركين بالإضافة إلى إصدار عناصر اعتماد مصداقيتهم. ربما يضم ذلك الكيان الهيئات المسئولة عن التسجيل وما تحتها من جهات التحقق من الهوية. كما يمكن أن يتمثل في طرف ثالث مستقل أو ربما يقوم بإصدار عناصر اعتماد المصداقية للاستخدام الخاص داخله فقط.	موفر خدمة عناصر اعتماد المصداقية	Credentials Service Provider (CSP) –

Security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and Personal Identification Numbers (PINs)) whose disclosure or modification can compromise the security of a cryptographic module.	معلومات تتعلق بالأمن مثل مفاتيح التشفير الخاصة والسرية وكذلك بيانات التصديق مثل كلمات المرور وأرقام التعريف الشخصية التي يؤدى الإفصاح عنها أو تغيرها إلى انتهاك الأمن الخاص بأحد وحدات التشفير النمطية.	معيار أمني حرج	Critical Security Parameter –
Refers to the (consequences of) incorrect behavior of a system. The more serious the expected direct and indirect effects of incorrect behavior, the higher the criticality level.	يشير إلى النتائج المترتبة على التصرف غير الصحيح لنظام معين. كلما زادت خطورة الآثار المباشرة أو غير المباشرة المتوقعة من ذلك التصرف غير الصحيح كلما زاد مستوى الدرجة الحرجة.	مستوى الدرجة الحرجة	Criticality Level –
A certificate used to establish a trust relationship between two Certification Authorities.	شهادة تستخدم لإقامة علاقة ثقة بين هيئتي توثيق.	شهادة الثقة المتبادلة	Cross-Certificate –
1) Operations performed in defeating cryptographic protection without an initial knowledge of the key employed in providing the protection.	1) عمليات تُنفَذ لكسر حماية التشفير بدون المعرفة المبدئية للمفتاح المُستخدم في توفير الحماية.		
2) The study of mathematical techniques for attempting to defeat cryptographic techniques and information system security. This includes the process of looking for errors or weaknesses in the implementation of an algorithm or of the algorithm itself.	2) دراسة لأساليب حسابية بغرض كسر طرق التشفير وأمن نظام المعلومات. يشمل ذلك عملية البحث عن أخطاء أو نقاط ضعف في تنفيذ خوارزمية معينة أو حتى في الخوارزمية نفسها.	كسر الشفرة	Cryptanalysis –
An operator or process (subject), acting on behalf of the operator, performing cryptographic initialization or management functions.	موظف أو عملية تقوم بالنيابة عن الموظف بتنفيذ إنشاء التشفير أو وظائف الإدارة.	موظف التشفير	Crypto Officer –
A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output.	إجراء حسابي مُعرَّف بدقة له مدخلات متغيرة بما في ذلك مفتاح تشفير معين و يُنتِج أحد المخرجات	خوارزمية التشفير	Cryptographic Algorithm –
An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.	حواجز متصلة ومُعرفَّة بوضوح لإقامة الحدود المادية لوحدة تشفير نمطية وتشمل كل الأجهزة والبرامج و/أو مكونات وحدة التشفير المثبتة في ذاكرة القراءة.	حدود التشفير	Cryptographic Boundary –
A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:	دالة تحول سلسلة نصية من وحدات البت ذات الطول العشوائي إلى سلسلة محددة الطول من وحدات البت. تتميز دالة الاختزال الصادر بشأنها موافقة بالمواصفات التالية:		
1) (One-way) It is computationally infeasible to find any input which maps to any pre-specified output, and	1) (وحيدة الاتجاه) بمعنى أنه من غير المُمكن رياضياً الحصول على مُدخَل يمكن تحويله إلى مُخرج محددة سلفاً و		
2) (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.	2) (مقاومة للتعارُض) فمن غير الممكن رياضياً الحصول على أي مدخلين مختلفين يتحولان إلى نفس المخرج.	التشفير باستخدام دالة الاختزال	Cryptographic Hash Function –

A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification. A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm. A parameter used in conjunction with a cryptographic algorithm that determines . the transformation of plaintext data into ciphertext data, . the transformation of ciphertext data into plaintext data, . a digital signature computed from data, . the verification of a digital signature computed from data, . an authentication code computed from data, or . an exchange agreement of a shared secret.	قيمة تُستخدم في العمليات التشفيرية مثل فك التشفير والتشفير وإصدار التوقيع أو التحقق من صحته. معيار يُستَخدم بالاقتران مع خوارزمية تشفير حيث يقوم بتحديد التشغيل المخصص لتلك الخوارزمية. معيار يُستَخدم مقترناً بخوارزمية تشفير لتحديد . تحويل البيانات من النص البسيط إلى نص مُشفر . تحويل النص المشفر إلى نص غير مُشفَّر . حساب التوقيع الالكتروني من البيانات . التحقق من صحة التوقيع الرقمي المحسوب من البيانات . شفرة التصديق المحسوبة من البيانات أو . اتفاقية تبادل لأحد الأسرار المشتركة.	مفتاح تشفير	Cryptographic Key –
The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. The set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.	مجموعة من الأجهزة أو البرامج أو برامج التشغيل المثبتة في ذاكرة القراءة أو خليط مما سبق لتنفيذ منطق أو عمليات التشفير بما في ذلك خوارزميات التشفير وتكون دائماً ضمن حدود التشفير الخاصة بالوحدة النمطية. مجموعة من الأجهزة والبرامج و/أو برامج التشغيل المثبتة في ذاكرة القراءة للقيام بتنفيذ وظائف أمنية صادر بشأنها موافقة بما في ذلك خوارزميات التشفير وإصدار المفاتيح وتكون ضمن حدود التشفير.	وحدة التشفير النمطية	Cryptographic Module –
A precise specification of the security rules under which a cryptographic module will operate, including the rules derived from the requirements of this standard (FIPS 140-2) and additional rules imposed by the vendor.	توصيف محدد لقواعد الأمن التي سوف تعمل من خلالها وحدة تشفير نمطية بما في ذلك القواعد المُستمَد من متطلبات معيار (FIPS 140-2) والقواعد الإضافية التي يفرضها البائع.	سياسة الأمن الخاص بوحدة التشفير النمطية	Cryptographic Module Security Policy –
Validates cryptographic modules to Federal Information Processing Standard (FIPS) 140-2 and other cryptography based standards. The CMVP is a joint effort between National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) of the Government of Canada. Products validated as conforming to FIPS 140-2 are accepted by the Federal agencies of both countries for the protection of sensitive information (United States) or Designated Information (Canada). The goal of the CMVP is to promote the use of validated cryptographic modules and provide Federal agencies with a security metric to use in procuring equipment containing validated cryptographic modules.	برنامج يثبت استيفاء وحدات التشفير النمطية لمعيار معالجة المعلومات الفيدرالي FIPS 140-2 ومعايير تشفير أخرى. هذا البرنامج نتاج الجهد المشترك بين المعهد الوطني للمقاييس والتقنية NIST ومؤسسة أمن الاتصالات CSE في الحكومة الكندية. المنتجات التي ثبت استيفائها لمعيار FIPS 140-2 يتم منحها الموافقة من الوكالات الفيدرالية في كلتا الدولتين بهدف حماية المعلومات الحساسة (من جهة الولايات المتحدة) أو المعلومات المحددة (من جهة كندا). الهدف من ذلك البرنامج هو تطوير استخدام وحدات التشفير النمطية المطابقة وتوفير مقياس أمني للوكالات الفيدرالية لاستخدامه في مشتريات الأجهزة التي تحتوى على وحدات تشفير نمطية سليمة.	برنامج إثبات صلاحية وحدات التشفير النمطية	Cryptographic Module Validation Program (CMVP) –
A measure of the expected number of operations required to defeat a cryptographic mechanism.	مقياس للعدد المتوقع من العمليات المطلوبة لكسر آلية من آليات التشفير.	قوة التشفير	Cryptographic Strength –
A token where the secret is a cryptographic key.	رمز مميز يكون السر فيه عبارة عن مفتاح تشفير.	رمز مميز للتشفير	Cryptographic Token –

The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification. The discipline that embodies principles, means and methods for providing information security, including confidentiality, data integrity, non-repudiation, and authenticity. It is categorized as either secret key or public key. Secret key cryptography is based on the use of a single cryptographic key shared between two parties . The same key is used to encrypt and decrypt data. This key is kept secret by the two parties. Public key cryptography is a form of cryptography which make use of two keys: a public key and a private key. The two keys are related but have the property that, given the public key, it is computationally infeasible to derive the private key [FIPS 140-1]. In a public key cryptosystem, each party has its own public/private key pair. The public key can be known by anyone; the private key is kept secret.	ذلك الفرع من فروع المعرفة الذي يهتم بتقديم مبادئ ووسائل وأساليب تحويل البيانات بغرض إخفاء ما تحويه من دلالات لفظية ومنع استخدامها دون تصريح وكذلك منع تغييرها. ذلك الفرع من المعرفة الذي يهتم بتقديم المبادئ والوسائل والأساليب التي توفر أمن المعلومات بما في ذلك السرية وتكامل البيانات وعدم الإنكار والمصداقية. وينقسم إلى مفتاح سري أو مفتاح عام. تشفير المفتاح السري يعتمد على استخدام مفتاح تشفير واحد مشترك بين طرفين. نفس المفتاح يستخدم في تشفير وفك تشفير البيانات. يحتفظ الطرفين بهذا المفتاح سراً . أما تشفير المفتاح العام فانه يستخدم مفتاحين أحدهما مفتاح عام والأخر مفتاح خاص. كلا المفتاحين مرتبط بالأخر ولكن للمفتاح العام خاصية وهي أنه لن يجدي اشتقاق المفتاح الخاص FIPS 140-1. في نظام تشفير المفتاح العام يمتلك كلا الطرفين زوج يضم مفتاح عام وأخر خاص. المفتاح العام متاح لأي شخص بينما يجب الاحتفاظ بسرية المفتاح الخاص.	التشفير	Cryptography –
The science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence.	هو ذلك العلم الذي يتعامل مع الاتصالات المخفية والمتنكرة والمشفرة ويضم أمن الاتصالات واستخبارات الاتصالات.	علم الشفرات	Cryptology –
Time span during which each key setting remains in effect.	الفترة التي تظل خلالها إعدادات المفتاح فعالة	فترة التشفير	Cryptoperiod –
A method to ensure data has not been altered after being sent through a communication channel.	أسلوب للتأكد من عدم تبديل البيانات بعد إرسالها من خلال قناة اتصال.	الفحص الدوري لأخطاء إرسال البيانات	Cyclical Redundancy Check (CRC) –
A basic unit of information that has a unique meaning and subcategories (data items) of distinct value. Examples of data elements include gender, race, and geographic location.	وحدة أساسية من المعلومات لها معنى فريد وفئات فرعية (عناصر بيانات) ذات قيمة مُعرَّفة بشكل مميز. من أمثلة عناصر البيانات النوع والسلالة والموقع الجغرافي.	عنصر بيانات	Data Element –
The cryptographic engine that is used by the Triple Data Encryption Algorithm (TDEA).	محرك تشفير يُستخدَم بواسطة خوارزمية التشفير الثلاثية للبيانات.	خوارزمية تشفير البيانات	Data Encryption Algorithm (DEA) –
A U.S. Government-approved, symmetric cipher, encryption algorithm used by business and civilian government agencies. The Advanced Encryption Standard (AES) is designed to replace DES. The original “single” DES algorithm is no longer secure because it is now possible to try every possible key with special purpose equipment or a high performance cluster. Triple DES, however, is still considered to be secure.	خوارزمية تشفير صادر بشأنها موافقة من حكومة الولايات المتحدة وتعتمد على الترميز المتناظر تُستخدَم بواسطة الشركات والوكالات الحكومية المدنية. وقد صُمِم المعيار المتقدم للتشفير ليحل محل معيار تشفير البيانات. لم تعد خوارزمية معيار تشفير البيانات المفرد آمنة والسبب أنه يمكن حالياً إجراء محاولات على كل مفتاح باستخدام أجهزة معينة أو وحدة تجميع عالية الأداء وبالرغم من ذلك يعتبر معيار التشفير الثلاثي للبيانات آمناً.	معيار تشفير البيانات	Data Encryption Standard (DES) –
The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.	خاصية عدم تغيير البيانات بطريقة غير مُصرَح بها. يغطى مفهوم التكامل البيانات في مرحلة تخزينها وأثناء معالجتها وأثناء مراحلها الانتقالية.	تكامل البيانات	Data Integrity –

The process of transforming ciphertext into plaintext. The process of changing ciphertext into plaintext using a cryptographic algorithm and key. Conversion of ciphertext to plaintext through the use of a cryptographic algorithm.	عملية تحويل نص التشفير إلى نص غير مُشفَّر. عملية تغيير نص تشفير إلى نص غير مُشفَّر باستخدام خوارزمية و مفتاح تشفير. تحويل نص تشفير إلى نص بسيط باستخدام خوارزمية تشفير	فك التشفير	Decryption –
A file that has been logically, but not necessarily physically, erased from the operating system, perhaps to eliminate potentially incriminating evidence. Deleting files does not always necessarily eliminate the possibility of recovering all or part of the original data.	ملف تم إزالته منطقياً – وليس بالضرورة مادياً – من نظام التشغيل ربما للتخلص من دليل يؤدى للتورط في جريمة. حذف الملفات لا يعنى بالضرورة فقدان إمكانية استرجاع كل البيانات الأصلية أو جزء منها.	ملف محذوف	Deleted File –
A network created by connecting two firewalls. Systems that are externally accessible but need some protections are usually located on DMZ networks.	شبكة مكونة من بربط اثنين من جدران الحماية. الأنظمة التي يتم الوصول إليها عن بعد ولكنها تحتاج لقدر من الحماية عادة ما توضع في شبكات المنطقة المحايدة.	منطقة محايدة	Demilitarized Zone (DMZ) –
The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)	منع الوصول المصرح به إلى الموارد أو تأخير العمليات التي يكون فيها الوقت عاملاً حرجاً. (ربما يقاس الوقت عندما يكون عاملاً حرجاً بالملي ثانية أو بالساعات اعتماداً على الخدمة المقدمة) .	تعطيل الخدمة	Denial of Service (DoS) –
The individual selected by an authorizing official to act on their behalf in coordinating and carrying out the necessary activities required during the security certification and accreditation of an information system.	الشخص الذي وقع عليه الاختيار من قبل موظف إصدار التصريح لكي ينوب عنه في التنسيق والقيام بالأنشطة الضرورية المطلوبة أثناء التوثيق الأمني واعتماد الموافقة لأحد أنظمة المعلومات.	نائب موظف إصدار التصريح	Designated Approving (Accrediting) Authority (DAA) –
The protocol used to assign Internet Protocol (IP) addresses to all nodes on the network.	بروتوكول يُستخدَم لإعطاء عناوين بروتوكول الانترنت لكل أجهزة الشبكة.	بروتوكول الإعداد الديناميكي للمضيف	Dynamic Host Configuration Protocol (DHCP) –
An analysis of the variations of the electrical power consumption of a cryptographic module, using advanced statistical methods and/or other techniques, for the purpose of extracting information correlated to cryptographic keys used in a cryptographic algorithm.	تحليل الاختلافات في استهلاك الطاقة الكهربية لوحدة تشفير نمطية باستخدام أساليب إحصائية متقدمة و/أو طرق أخرى بغرض استخلاص المعلومات المتعلقة بمفاتيح التشفير المُستخدمة في خوارزمية تشفير معينة.	تحليل التباين في القوة	Differential Power Analysis (DPA) –
Electronic information stored or transferred in digital form. An asymmetric key operation where the private key is used to digitally sign an electronic document and the public key is used to verify the signature. Digital signatures provide authentication and integrity protection. A nonforgeable transformation of data that allows the proof of the source (with nonrepudiation) and the verification of the integrity of that data. The result of a cryptographic transformation of data which, when properly implemented, provides the services of:	المعلومات الالكترونية المخزنة أو المنقولة في شكل رقمي. عملية تعتمد على مفتاح غير متناظر حيث يتم استخدام المفتاح الخاص للتوقيع رقمياً على وثيقة الكترونية بينما يقوم المفتاح العام بالتحقق من صحة ذلك التوقيع. التوقيعات الالكترونية توفر إمكانية التحقق من الهوية وحماية التكامل. تحويل للبيانات غير قابل للنسيان حيث يسمح بإثبات مصدر البيانات (بلا أي إنكار) وكذلك التحقق من تكاملها. النتيجة المترتبة على التحويل المُشَفَر للبيانات والذي إن تم تطبيقه بطريقة صحيحة يوفر الخدمات التالية:		
1. origin authentication	1. التحقق من المصدر		
2. data integrity, and	2. صحة البيانات وتكاملها		
3. signer non-repudiation.	3. عدم قدرة المُوَقِع على الإنكار.	الدليل الرقمي	Digital Evidence –

Asymmetric algorithms used for digitally signing data.	خوارزميات غير متناظرة تُستخدَم لتوقيع البيانات رقمياً.	خوارزمية التوقيع الرقمي	Digital Signature Algorithm –
A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.	خطة مكتوبة لمعالجة التطبيقات الحرجة في حالة تعطل الأجهزة والبرامج الرئيسية أو تعرض المنشآت للدمار.	خطة معالجة الكوارث	Disaster Recovery Plan (DRP) –
The termination of an interconnection between two or more IT systems. A disconnection may be planned (e.g., due to changed business needs) or unplanned (i.e., due to an attack or other contingency).	إنهاء الاتصال المتبادلة بين اثنين أو أكثر من أنظمة تقنية المعلومات. قطع الاتصال من الممكن أن يكون مخطط له (على سبيل المثال نتيجة لتغير احتياجات العمل) أو غير مخطط له (على سبيل المثال نتيجة هجوم أو أية طوارئ أخرى)	قطع الاتصال	Disconnection –
The basis of this kind of security is that an individual user, or program operating on the user’s behalf is allowed to specify explicitly the types of access other users (or programs executing on their behalf) may have to information under the user’s control.	الأساس الذي يقوم عليه هذا النوع من الأمن هو أن المستخدم أو برنامج التشغيل نيابة عن المستخدم مسموح له أن يحدد بوضوح أنواع وصول المستخدمين الآخرين (أو البرامج المنفذة التي تنوب عنهم) إلى المعلومات التي تقع تحت سيطرته	التحكم النسبي في الوصول	Discretionary Access Control –
An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).	حدث غير مخطط له يتسبب في توقف النظام العمومي أو التطبيقات الرئيسية لفترة غير مقبولة من الزمن (على سبيل المثال انقطاع التيار الكهربي لفترة قد تكون قصيرة أو تمتد أو عدم توفر شبكة الاتصالات لفترة طويلة أو تعرض الأجهزة والمنشأة إلى التلف أو الدمار)	خلل	Disruption –
Information which unambiguously distinguishes an entity in the authentication process.	المعلومات التي تميز كيان بعينه دون التباس في عملية التصديق للتحقق من الهوية	عنصر التعريف المُميِّز	Distinguishing Identifier –
A Denial of Service technique that uses numerous hosts to perform the attack.	أسلوب لحجب الخدمة باستخدام العديد من أجهزة المضيف بغرض تنفيذ الهجوم	حجب الخدمة الموزَّع	Distributed Denial of Service (DDoS) –
A set of subjects, their information objects, and a common security policy.	مجموعة من الأطراف الفاعلة وعناصر معلوماتها بالإضافة إلى سياسة أمن مشترك	مجال / نطاق	Domain –
A certificate that is intended for use with both digital signature and data encryption services.	شهادة يُقصد لها أن تستخدم في خدمات كلاً من التوقيع الالكتروني وتشفير البيانات	شهادة مزدوجة الاستخدام	Dual-Use Certificate –
The responsibility that managers and their organizations have a duty to provide for information security to ensure that the type of control, the cost of control, and the deployment of control are appropriate for the system being managed.	مسؤولية المديرين ومنظماتهم تجاه الالتزام بتوفير أمن المعلومات للتأكد من أن نوع التحكم وتكلفته وكذلك تطبيقه يتناسب مع النظام المُدار	الاهتمام المناسب	Due Care –
A duplicate is an accurate digital reproduction of all data objects contained on the original physical item and associated media.	إعادة إنتاج رقمي دقيق لكل البيانات الموجودة على الجهاز الأصلي وما يتعلق به من وسائط	نسخة طبق الأصل من الأدلة الرقمية	Duplicate Digital Evidence –
A field within a certificate that is composed of two subfields; “date of issue” and “date of next issue”.	حقل بيانات في شهادة ينقسم إلى حقلين فرعيين هما "تاريخ الإصدار" و"تاريخ الإصدار التالي"	مدة الصلاحية	Duration –

Hidden functionality within an application program, which becomes activated when an undocumented, and often convoluted, set of commands and keystrokes are entered. Easter eggs are typically used to display the credits for the development team and are intended to be non-threatening.	تعبير مجازي عن وظيفة أو امكانية مخفية فى التطبيق تصبح نشطة عند إدخال مجموعة من الاوامر أو الضغط على توليفة من المفاتيح عادةً ما تكون غير موثَّقة أو بالأحرى تكون معقدة. تستخدم "بيضة الفصح" بشكل نموذجي لعرض البيانات الخاصة بفريق تطوير دون أن تسبب أى تهديد.	"بيضة الفصح"	Easter Egg –
Education integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge . . . and strives to produce IT security specialists and professionals capable of vision and pro-active response.	تعليم يضم كل مهارات وقدرات الأمن من عدة تخصصات وظيفية داخل إطار عام من المعرفة... ويسعى لإخراج متخصصين ومحترفين في مجال الأمن يكون لديهم الرؤية والاستجابة السريعة	تعليم أمن المعلومات	Information Security Education –
The process of blocking outgoing packets that use obviously false Internet Protocol (IP) addresses, such as source addresses from internal networks.	عملية منع حزم البيانات التي يكون من الواضح استخدامها لعناوين انترنت وهمية مثل عناوين المصدر من الشبكات الداخلية	تصفية العناوين الوهمية	Egress Filtering –
The process of establishing confidence in user identities electronically presented to an information system.	عملية إثبات الثقة في هويات المستخدمين المقدمة الكترونياً لنظام معلومات	التصديق الالكتروني / التحقق من الهوية الكترونياً	Electronic Authentication (E-authentication) –
Digital documents used in authentication that bind an identity or an attribute to a subscriber's token.	وثائق الكترونية تُستخدَم للتصديق تقوم بربط الهوية أو أحد الخواص بالرمز المميز للمشترك	عناصر اعتماد المصداقية الالكترونية	Electronic Credentials –
Information and data of investigative value that is stored on or transmitted by an electronic device.	معلومات وبيانات لها قيمة في عملية التحريات وتُخزَّن في أو تُنقَّل بواسطة وسيلة إلكترونية	الأدلة الالكترونية	Electronic Evidence –
The entry of cryptographic keys into a cryptographic module using electronic methods such as a smart card or a key-loading device. (The operator of the key may have no knowledge of the value of the key being entered.)	مدخل مفاتيح التشفير إلى وحدة التشفير النمطية باستخدام أساليب إلكترونية مثل البطاقات الذكية أو وسائل تحميل المفتاح (ربما لا يملك مُشَغِّل المفتاح المعرفة بقيمة المفتاح المُدخل)	مدخل المفتاح الالكتروني	Electronic Key Entry –
A cryptographic key that has been encrypted using an approved security function with a key encrypting key, a PIN, or a password in order to disguise the value of the underlying plaintext key.	مفتاح تشفير تم تشفيره باستخدام دالة أمنية صادر بشأنها موافقة مع مفتاح تشفير أساسي أو رقم تعريف شخصي أو كلمة مرور بغرض إخفاء القيمة الأساسية للنص غير المُشفَّر للمفتاح	مفتاح مُشفَّر	Encrypted Key –
A network on which messages are encrypted (e.g. using DES, AES, or other appropriate algorithms) to prevent reading by unauthorized parties.	شبكة تكون الرسائل فيها مُشفَّرة (على سبيل المثال باستخدام معيار تشفير البيانات أو المعيار المتقدم للتشفير أو غيرها من الخوارزميات المناسبة) لمنع الأطراف غير المصرح لها من القراءة	شبكة مُشفَّرة	Encrypted Network –
Encryption is the conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorized people. Conversion of plaintext to ciphertext through the use of a cryptographic algorithm. The process of changing plaintext into ciphertext for the purpose of security or privacy.	هو تحويل البيانات إلى شكل يسمى نص الترميز حيث لا يمكن فهمه بسهولة من خلال الأشخاص غير المصرّح لهم. تحويل النص غير المُشفَّر إلى نص الترميز من باستخدام خوارزمية تشفير. تحويل النص غير المُشفَّر إلى نص الترميز لأغراض السرية والأمن	التشفير	Encryption –
A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.	شهادة تحتوى على مفتاح عام يُستخدَم في تشفير الرسائل الالكترونية أو الملفات أو المستندات أو عمليات نقل البيانات بالإضافة إلى إنشاء أو تبديل مفتاح خاص بفترة التعامل مع النظام لنفس الأغراض	شهادة التشفير	Encryption Certificate –

Communications encryption in which data is encrypted when being passed through a network, but routing information remains visible.	تشفير الاتصالات الذي تكون فيه البيانات مُشفَّرة عند نقلها عبر الشبكة مع الاحتفاظ معلومات التوجيه مرئية	تشفير النهايات	End to End Encryption –
Either a subject (an active element that operates on information or the system state) or an object (a passive element that contains or receives information). An active element in an open system. Any participant in an authentication exchange; such a participant may be human or nonhuman, and may take the role of a claimant and/or verifier.	إما أن يكون فاعل (بمعنى أنه عنصر فعَّال يؤدي بعض العمليات على المعلومات أو حالة النظام) أو أنه مفعول (بمعنى أنه عنصر سلبي يحتوى أو يستقبل المعلومات). عنصر فعَال في نظام مفتوح. أي طرف مشارك في تبادل التصديق. هذا الطرف يُحتمَل أن يكون بشر أو غير بشر وربما يلعب دور مقدم الطلب أومن يقوم بالتحقق من صحة الهوية	كيان	Entity –
A measure of the amount of uncertainty that an attacker faces to determine the value of a secret.	مقياس لمدى الشك الذي يواجهه المهاجم لتحديد قيمة أحد الأسرار	معامل الشك	Entropy –
Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an information system.	مجموع الإجراءات والظروف والعناصر الخارجية التي تؤثر على تطوير وعمل وصيانة نظام معلومات	بيئة	Environment –
Short-lived cryptographic keys that are statistically unique to each execution of a key establishment process and meets other requirements of the key type (e.g., unique to each message or session).	مفاتيح تشفير قصيرة الأجل من الناحية الإحصائية لا تقبل التكرار عند إجراء عملية إنشاء أحد المفاتيح كما أنها تلبى المتطلبات الأخرى لنوع المفتاح (مثل أن يكون المفتاح فريداً لكل رسالة أو جلسة عمل)	مفاتيح قصيرة الأجل	Ephemeral Keys –
A code computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data.	شفرة تُحسب من البيانات وتتكون من معلومات فائضة مصمَمة لاكتشاف وليس لتصحيح التغييرات التي تحدث في البيانات بشكل غير مقصود	شفرة اكتشاف الأخطاء	Error Detection Code –
Something (e.g., a document, an encryption key) that is "delivered to a third person to be given to the grantee only upon the fulfillment of a condition."	شيء (مستند أو مفتاح تشفير مثلاً) يُودَع لدى طرف ثالث بغرض إعطاءه للطرف الضامن فقط عند وفاءه بشرط معين	ضمان / تأمين	Escrow –
Any observable occurrence in a network or system.	أي حدث يسترعى الملاحظة في الشبكة أو النظام	حدث	Event –
A technical review that makes the evidence visible and suitable for analysis; tests performed on the evidence to determine the presence or absence of specific data.	مراجعة فنية بغرض جعل الأدلة مرئية ومناسبة للتحليل ثم تُجرى الاختبارات على الأدلة لتحديد وجود أو فقدان بيانات معينة	فحص	Examination –
Evidence that tends to decrease the likelihood of fault or guilt.	دليل يميل إلى تقليل احتمالية الخطأ أو الذنب	دليل ترجيح البراءة	Exculpatory Evidence –
An executive department specified in 5 United States Code (U.S.C.), Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.	إدارة تنفيذية محددة في التبويب الخامس لقانون الولايات المتحدة طبقاً للمقطع 101 . شعبة عسكرية محددة في التبويب الخامس قانون الولايات المتحدة طبقاً للمقطع 102 . مؤسسة مستقلة محددة في التبويب الخامس قانون الولايات المتحدة طبقاً للمقطع 104 . مؤسسة مملوكة بالكامل للحكومة تخضع لأحكام الباب 31 من قانون الولايات المتحدة فصل 91 .	وكالة تنفيذية	Executive Agency –
A program that allows attackers to automatically break into a system.	برنامج يسمح للمهاجمين باقتحام النظام آلياً	شفرة الاقتحام	Exploit Code –
When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity	عندما يقوم نظام للقياسات الحيوية بتعريف شخص بطريقة خاطئة أو يرتكب خطأ في التحقق من محتال يدعى هوية معينة	القبول الخاطئ	False Acceptance –

The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts.	احتمالية أن يقوم نظام القياسات الحيوية خطأً بالتعرف على شخص أو أن يفشل في رفض هوية شخص محتال. المعدل يفترض في العادة أن تكون كل محاولات الاحتيال كامنة	معدل القبول الخاطئ	False Acceptance Rate –
Alternative to ‘False Acceptance Rate’. Used to avoid confusion in applications that reject the claimant if their biometric data matches that of an applicant.	بديل لـ "معدل القبول الخطأ" يُستَخدم في تجنب إثارة الارتباك في التطبيقات التي ترفض المُدَّعى إذا ما كانت بيانات قياساتها الحيوية تطابق تلك الخاصة بالمشترك	معدل التطابق الخاطئ	False Match Rate (FMR) –
Alternative to ‘False Rejection Rate’. Used to avoid confusion in applications that reject the claimant if their biometric data matches that of an applicant.	بديل لـ "معدل الرفض الخطأ" يُستخدم في تجنب إثارة الارتباك في التطبيقات التي ترفض المدعى إذا ما كانت بيانات قياساتها الحيوية تطابق تلك الخاصة بالمشترك	معدل عدم المطابقة الخاطئة	False Non Match Rate (FNMR) –
An alert that incorrectly indicates that malicious activity is occurring.	إنذار يشير بطريقة خاطئة إلى حدوث نشاط خبيث	إنذار خاطئ	False Positive –
When a biometric system fails to identify an applicant or fails to verify the legitimate claimed identity of an applicant.	هي تلك الحالة التي يفشل فيها نظام قياسات حيوي في التعرف على المشترك أو في التحقق من شرعية الهوية التي يدعيها المشترك	رفض خاطئ	False Rejection –
The probability that a biometric system will fail to identify an applicant, or verify the legitimate claimed identity of an applicant.	احتمالية فشل نظام قياس حيوي في التعرف على مشترك أو التحقق من شرعية الهوية التي يدعيها مشترك	معدل الرفض الخاطئ	False Rejection Rate (FRR) –
The Federal Bridge Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer-to-peer interoperability among Agency Principal Certification Authorities.	تتكون الهيئة الفيدرالية المشتركة للتوثيق من مجموعة مكونات للبنية التحتية للمفتاح العام (هيئات التوثيق والأدلة وسياسات الشهادات وبيانات الممارسة الخاصة بالشهادات) التي تُستخدَم في توفير خدمة "الند للند" بين هيئات التوثيق الرئيسية في الوكالة	الهيئة الفيدرالية المشتركة للتوثيق	Federal Bridge Certification Authority (FBCA) –
The Federal Bridge Certification Authority Membrane consists of a collection of Public Key Infrastructure components including a variety of Certification Authority PKI products, Databases, CA specific Directories, Border Directory, Firewalls, Routers, Randomizers, etc.	يضم إطار الهيئة الفيدرالية المشتركة للتوثيق مجموعة من مكونات البنية التحتية للمفتاح العام التي تشمل مجموعة متنوعة من منتجات تلك البنية التي تَصدُر عن هيئة التوثيق بالإضافة إلى قواعد بيانات وأدلة خاصة بهيئة التوثيق والأدلة الخارجية وجدران الحماية والموجهات ومولدات القيم العشوائية وغيرها	إطار الهيئة الفيدرالية المشتركة للتوثيق	Federal Bridge Certification Authority Membrane –
The Federal Bridge Certification Authority Operational Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.	هي تلك الجهة التي اختارتها هيئة سياسات البنية التحتية للمفتاح العام لكي تكون مسؤولة عن تشغيل الهيئة الفيدرالية المشتركة للتوثيق	إدارة تشغيل الهيئة الفيدرالية المشتركة للتوثيق	Federal Bridge Certification Authority Operational Authority –
A standard for adoption and use by Federal agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability.	معيار تتبناه وتستخدمه الوكالات الفيدرالية حيث تم تطويره داخل "معمل تقنية المعلومات" وقام بنشره المعهد الوطني للمقاييس والتقنية التابع لوزارة التجارة الأمريكية. يغطى هذا المعيار بعض الموضوعات المتعلقة بتقنية المعلومات لتحقيق مستوى عام من الجودة وبعض الشيء من العمل المشترك	المعيار الفيدرالي لمعالجة المعلومات	Federal Information Processing Standard (FIPS) –

An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.	نظام معلومات يُستخدَم أو يُشغَّل بواسطة وكالة تنفيذية أو أحد المتعاقدين مع وكالة تنفيذية أو أية منظمة أخرى تعمل نيابةً عن وكالة تنفيذية.	نظام معلومات فيدرالي	Federal Information System –
An organization whose members come from federal agencies, industry, and academic institutions devoted to improving the IT security awareness and knowledge within the federal government and its related external workforce.	منظمة يأتي أعضاءها من الوكالات الفيدرالية والصناعة والمعاهد الأكاديمية تختص بتحسين الوعي حول أمن تقنية المعلومات وزيادة المعرفة به داخل الحكومة الفيدرالية وأماكن العمل الخارجية التابعة لها.	رابطة مُعلِّمي أمن أنظمة المعلومات الفيدرالية	Federal Information Systems Security Educators' Association (FISSEA) –
The Federal PKI Policy Authority is a federal government body responsible for setting, implementing, and administering policy decisions regarding interagency PKI interoperability that uses the FBCA.	جهاز حكومي فيدرالي مسؤول عن وضع وتنفيذ وإدارة قرارات سياسة العمل المشترك القائم على البنية التحتية للمفتاح العام بين الوكالات ويستخدم إدارة تشغيل الهيئة الفيدرالية المشتركة للتوثيق.	الهيئة الفيدرالية لسياسة البنية التحتية للمفتاح العام	Federal Public Key Infrastructure Policy Authority (FPKI PA) –
A virus that attaches itself to a program file, such as a word processor, spreadsheet application, or game.	فيروس يلصق نفسه بملف أحد البرامج مثل ملفات برامج معالجة الكلمات وبرامج الحسابات والألعاب.	فيروس ملفات البرامج	File Infector Virus –
Software that generates, stores, and compares message digests for files to detect changes to the files.	برنامج يقوم بإصدار وتخزين ومقارنة موجز الرسائل الخاصة بالملفات لاكتشاف التغييرات التي حدثت في تلك الملفات.	فاحص تكامل الملفات	File Integrity Checker –
1) A mismatch between the internal file header and its external extension; 2) A file name inconsistent with the content of the file (e.g., renaming a graphics file with a non-graphical extension.	1) عدم تطابق بين ترويسة الملف الداخلية و امتداده الخارجي 2) اسم ملف غير مطابق لمحتواه (على سبيل المثال إعادة تسمية ملف رسوميات بامتداد غير مطابق للرسوميات)	اسم ملف غير مطابق	File Name Anomaly –
A security method (e.g., cryptographic algorithm, cryptographic key generation algorithm or key distribution technique, random number generator, authentication technique, or evaluation criteria) that is either a) specified in a FIPS, or b) adopted in a FIPS.	أسلوب أمن (على سبيل المثال خوارزمية تشفير أو خوارزمية إصدار مفاتيح تشفير أو طريقة توزيع المفتاح أو مولد أرقام عشوائية أو طريقة تحقق من الهوية أو معيار تقييم) حدده أو أقره المعيار الفيدرالي لمعالجة البيانات.	أسلوب أمني صادر بشأنه موافقة طبقاً للمعيار الفيدرالي لمعالجة البيانات	FIPS Approved Security Method –
An acronym for Federal Information Processing Standards Publication. FIPS publications (PUB) are issued by NIST after approval by the Secretary of Commerce.	اختصار لـ "منشورات المعيار الفيدرالي لمعالجة المعلومات" . تصدر تلك النشرات عن المعهد الوطني للمقاييس والتقنية بعد اعتماد الموافقة عليها من وزير التجارة.	نشرات المعيار الفيدرالي لمعالجة البيانات	FIPS PUB –
A gateway that limits access between networks in accordance with local security policy.	بوابة تتحكم في الوصول بين الشبكات طبقاً لسياسة الأمن المحلية .	جدار حماية	Firewall –
The component that controls a firewall's handling of a call. The firewall control proxy can instruct the firewall to open specific ports that are needed by a call, and direct the firewall to close these ports at call termination.	أحد المكونات التي تتحكم في تعامل جدار الحماية مع طلبات الاتصال حيث يستطيع وكيل التحكم أن يصدر أمراً لجدار الحماية بفتح منافذ محددة يتطلبها إجراء الاتصال وإغلاق تلك المنافذ عند إنهاء الاتصال.	وكيل التحكم الخاص بجدار الحماية	Firewall Control Proxy –
A firewall environment is a collection of systems at a point on a network that together constitute a firewall implementation. A firewall environment could consist of one device or many devices such as several firewalls, intrusion detection systems, and proxy servers.	بيئة جدار الحماية هي مجموعة أنظمة في مكان معين من الشبكة تشكل معاً تطبيقاً لجدار حماية. تلك البيئة يمكن أن تتكون من جهاز واحد أو عدة أجهزة على سبيل المثال عدة جدران حماية وأنظمة لاكتشاف الاختراق وخوادم وكيله.	بيئة جدار الحماية	Firewall Environment –

A firewall platform is the system device upon which a firewall is implemented. An example of a firewall platform is a commercial operating system running on a personal computer.	هي أحد أجهزة النظام الذي يتم تنفيذ جدار الحماية عليه مثال لذلك نظام التشغيل المثبت على الحاسوب الشخصي.	منصة جدار الحماية	Firewall Platform –
A firewall ruleset is a table of instructions that the firewall uses for determining how packets should be routed between its interfaces. In routers, the ruleset can be a file that the router examines from top to bottom when making routing decisions.	جدول تعليمات يستخدمه جدار الحماية لتحديد كيفية توجيه حزم البيانات بين قنوات الاتصال. داخل أجهزة الموجه يمكن أن يكون جدول التوجيه ملف يقوم الموَجِّه بالبحث فيه من الأعلى لأسفل عند اتخاذ قرارات توجيه حزم البيانات.	تعليمات توجيه البيانات في جدار الحماية	Firewall Ruleset –
The programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution.	البرامج ومكونات البيانات الخاصة بوحدة تشفير نمطية محفوظة على جهاز داخل حدود التشفير ولا يمكن الكتابة عليها أو تغييرها ديناميكياً أثناء التنفيذ.	برامج التشغيل المثبتة في ذاكرة القراءة	Firmware –
Federal Information Security Management Act - requires agencies to integrate IT security into their capital planning and enterprise architecture processes at the agency, conduct annual IT security reviews of all programs and systems, and report the results of those reviews to the Office of Management and Budget (OMB).	قانون إدارة أمن المعلومات الفيدرالي يطالب الوكالات بضم أمن تقنية المعلومات إلى تخطيط رأس المال وعمليات الهيكلة المؤسسية للوكالة بالإضافة إلى إجراء مراجعات سنوية لكل البرامج والأنظمة فيما يخص أمن تقنية المعلومات ورفع تقرير بنتائج تلك المراجعات إلى مكتب الإدارة والميزانية.	قانون إدارة أمن المعلومات الفيدرالي	FISMA –
An accurate bit-for-bit reproduction of the information contained on an electronic device or associated media, whose validity and integrity has been verified using an accepted algorithm.	إعادة دقيقة لإنتاج المعلومات الموجودة على أحد الأجهزة الالكترونية أو أحد الوسائط الملحقة التي يجري التحقق من صلاحيتها وتكاملها باستخدام خوارزمية مقبولة.	نسخة طبق الأصل	Forensic Copy –
A professional who locates, identifies, collects, analyzes and examines data while preserving the integrity and maintaining a strict chain of custody of information discovered.	شخص محترف يقوم بتعيين وتعريف وجمع وتحليل وفحص البيانات مع المحافظة على التكامل وإتباع سلسلة من التحفظ على ما يُكتَشَف من معلومات.	متخصص في علم الأدلة الجنائية	Forensic Specialist –
The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.	جمع البيانات الخاصة بالحاسوب والاحتفاظ بها وتحليلها من أجل أغراض تقصى حقائق بطريقة تحافظ على تكامل البيانات.	التحليل الجنائي لبيانات الحاسوب	Forensics, Computer –
The function that transforms the payload, associated data, and nonce into a sequence of complete blocks.	وظيفة لتحويل البيانات المرسلة عبر الشبكة و البيانات المرتبطة بها إلى سلسلة قوالب كاملة	وظيفة التنسيق	Formatting Function –
One of the two functions of the block cipher algorithm that is determined by the choice of a cryptographic key.	أحد وظيفتين من وظائف خوارزمية قالب الترميز يتم تحديدها باختيار مفتاح تشفير.	وظيفة الترميز الأمامي	Forward Cipher –
An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.	مجموعة مترابطة من موارد المعلومات تخضع لنفس التحكم الإداري المباشر وتتشارك في النواحي الوظيفية وتشتمل عادة على أجهزة وبرامج ومعلومات وبيانات وتطبيقات واتصالات وأشخاص.	نظام الدعم العام	General Support System –
A security system that provides several levels (e.g., low, moderate, high) of protection based on threats, risks, available technology, support services, time, human concerns, and economics.	نظام أمني يوفر مستويات متعددة من الحماية (منخفضة ومتوسطة ومرتفعة) بناءاً على التهديدات والمخاطر والتقنية المتوفرة وخدمات الدعم والوقت والنواحي البشرية والاقتصادية.	الأمن المتدرج	Graduated Security –

A mechanism limiting the exchange of information between information systems or subsystems.	آلية تعمل على الحد من تبادل المعلومات بين أنظمة المعلومات أو الأنظمة الفرعية.	حرس النظام	Guard (System) –
A measure of the difficulty that an attacker has to guess the average password used in a system. In this document, entropy is stated in bits. When a password has n-bits of guessing entropy then an attacker has as much difficulty guessing the average password as in guessing an n-bit random quantity. The attacker is assumed to know the actual password frequency distribution.	مقياس للصعوبة التي يواجهها المهاجم لتخمين كلمة المرور المستخدمة في نظام معين. في هذه الوثيقة يتم حساب معامل صعوبة التخمين بوحدات البت بمعنى أنه إذا كانت كلمة المرور لها معامل تخمين يُقدَّر بعدد معين من وحدات البت فإن المهاجم تواجهه صعوبة في تخمين كلمة المرور تقدر بمحاولته التخمين في مقدار عشوائي يساوي ذلك العدد. من المفترض أن يكون المهاجم على علم بمرات توزيع كلمة المرور الحقيقة.	معامل صعوبة التخمين	Guessing Entropy –
A type of program used in DDoS attacks to control agents distributed throughout a network. Also refers to an incident handler, which refers to a person who performs incident response work.	نوع من البرامج يُستخدَم في هجمات حجب الخدمة الموزَّعَة للسيطرة على عملاء موزعين في أنحاء الشبكة. كما يشير أيضاً لمعالج التحكم الخاص بالحدث حيث يعبر عن شخص يقوم بعمل إجابة للحدث.	معالج تحكم	Handler –
A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:	دالة تحول سلسلة نصية من وحدات البت ذات الطول غير المحدد إلى سلسلة محددة الطول من وحدات البت. تتميز دالة الاختزال الصادر بشأنها موافقة بالمواصفات التالية:		
1) One-Way. It is computationally infeasible to find any input that maps to any pre-specified output.	1) (وحيدة الاتجاه) بمعنى أنه من غير المُمكن حسابياً يتحول مدخل إلى مخرج محدد سلفاً و		
2) Collision Resistant. It is computationally infeasible to find any two distinct inputs that map to the same output. An approved mathematical function that maps a string of arbitrary length (up to a pre-determined maximum size) to a fixed length string. It may be used to produce a checksum, called a hash value or message digest, for a potentially long string or message.	2) (مقاومة للتعارُض) بمعنى أنه من غير الممكن حسابياً أن يتحول مدخلان مختلفان إلى نفس المخرج. دالة حسابية صادر بشأنها موافقة تقوم بتحويل سلسلة نصية ذات طول غير محدد إلى سلسلة نصية محددة الطول. يمكن استخدامها لإنتاج مجموع تدقيقي يُسمّى بـ "قيمة الاختزال" أو"موجز الرسالة" لسلسلة نصية أو رسالة طويلة.	دالة الاختزال	Hash Function –
A symmetric key authentication method using hash functions. A message authentication code that uses a cryptographic key in conjunction with a hash function. A message authentication code that utilizes a keyed hash.	أسلوب تصديق ذو مفتاح متناظر يستخدم دوال اختزال. شفرة رسالة تصديق تستخدم مفتاح تشفير مرتبط بدالة اختزال. شفرة رسالة تصديق تستخدم اختزال مُشفَّر بمفتاح.	شفرة التصديق الخاصة بالرسالة المعتمدة على الاختزال	Hash-based Message Authentication Code (HMAC) –
The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.	عملية تطبيق خوارزمية حسابية على بيانات للحصول على قيمة عددية تعبر عن تلك البيانات.	خوارزمية الاختزال	Hashing –
An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.	جهاز حماية حدود نقطة اتصال يتحكم في إمكانية الوصول بين شبكة محلية تتطلب وجود حماية بواسطة نظام مؤسسي وبين شبكة خارجية لا تخضع لتحكم النظام المؤسسي مع درجة عالية من التأمين.	حرس عالي التأمين	High Assurance Guard (HAG) –
An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.	نظام معلومات يكون فيه على الأقل هدف أمني واحد (السرية أو التكامل أو استمرارية توفر الخدمة) قد تم منحه درجة "عالي" طبقاً للمعيار الفيدرالي لمعالجة البيانات رقم 199 الخاص بالتأثير المحتمل.	نظام عالي التأثير	High Impact System –

A host that is designed to collect data on suspicious activity and has no authorized users other than its administrators.	جهاز مضيف مُصمَم لجمع البيانات حول الأنشطة المثيرة للريبة التي يتعرض لها النظام وليس لأي مستخدم تصريح باستعماله إلا مديري ذلك الجهاز.	جهاز المضيف المخادع	Honeypot –
A fully operational off-site data processing facility equipped with hardware and system software to be used in the event of a disaster.	منشأ لمعالجة البيانات تعمل بكامل قوتها التشغيلية بعيداً عن الموقع الرئيسي للنظام. تكون مُجهزَة بالأجهزة والبرامج لاستخدامها في حالات الكوارث.	موقع ساخن	Hot Site –
The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items.	إجراءات للتحقق من هوية مستخدم أو عملية أو جهاز تُمثِل عادة أحد الشروط المسبقة للحصول على حق الوصول إلى أحد الموارد في نظام لتقنية المعلومات. إجراءات اكتشاف الهوية الحقيقية (على سبيل المثال المصدر والبيانات التاريخية المبدئية) لشخص أو عنصر من مجموعة تضم أشخاص أو عناصر متشابهة.	كشف الهوية	Identification –
A unique data string used as a key in the biometric system to name a person’s identity and its associated attributes.	سلسلة نصية من البيانات الفريدة تُستخدَم كمفتاح في نظام قياسات حيوية لتحديد هوية شخص وما يتعلق بها من خصائص.	عنصر تعريف	Identifier –
A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information to make the complete name unique.	أسم شخص غير قابل للتكرار لكن الأسماء الشخصية عادة ما تتكرر لذلك فإن هوية الشخص يجب أن تضم معلومات إضافية بشكل كافٍ يجعل الاسم الكامل غير قابل للتكرار. مجموعة الصفات البدنية والسلوكية التي تجعل من شخص ما معروفاً بشكل غير قابل للتكرار.	الهوية	Identity –
A security policy based on the identities and/or attributes of the object (system resource) being accessed and of the subject (user, group of users, process, or device) requesting access.	سياسة أمن تعتمد على الهويات و/أو الخواص المميزة للمفعول (أحد موارد النظام) الذي يتم الوصول إليه والفاعل (مستخدم ، مجموعة مستخدمين ، عملية ، جهاز) الذي يطلب الوصول.	سياسة أمن تقوم على الهوية	Identity-Based Security Policy –
Binding of the vetted claimed identity to the individual (through biometrics) according to the issuing authority.	ربط ما تم فحصه من هوية مدَّعاة بالشخص (من خلال القياسات الحيوية) طبقاً للهيئة المُصدرَة للهوية.	ربط الهوية	Identity Binding –
The process by which a Credentials Service Provider (CSP) and a Registration Authority (RA) validate sufficient information to uniquely identify a person. The process of providing sufficient information (e.g., identity history, credentials, documents) to a Personal Identity Verification Registrar when attempting to establish an identity.	العملية التي يقوم فيها موفر خدمة عناصر اعتماد المصداقية وهيئة التسجيل بالتحقق من وجود المعلومات الكافية التي تحدد هوية شخص بشكل فريد لا يتكرر. عملية توفير معلومات كافية (مثل البيانات التاريخية للشخصية وعناصر اعتماد المصداقية والمستندات) إلى سجل التحقق من صحة الهوية الشخصية عند العمل على استخراج هوية شخصية.	إثبات الهوية	Identity Proofing –
The process of making a person’s identity known to the Personal Identity Verification (PIV) system, associating a unique identifier with that identity, and collecting and recording the person’s relevant attributes into the system.	عملية نشر هوية الشخص على نظام التحقق من صحة الهوية الشخصية من خلال ربط عنصر تعريف غير قابل للتكرار بالهوية وتجميع وتسجيل الخواص المتعلقة بالشخص في النظام.	تسجيل الهوية	Identity Registration –

Identity Verification –	التحقق من الهوية	التأكد من صحة هوية مدعاة عن طريق المقارنة بين إدعاءات الهوية المقدمة والمعلومات الثابتة مسبقاً والمخزنة ً في بطاقة الهوية أو نظام التحقق من صحة الهوية الشخصية. تأكيد أو إنكار صحة الهوية التي تم إدعاءها من خلال مقارنة عناصر اعتماد المصداقية (شيء تعرفه أو تمتلكه أو يحدد صفة) لشخص يطلب الوصول بالبيانات الصحيحة التي تكون مخزنة في بطاقة أو نظام التحقق من الهوية الشخصية ومربوطة بالهوية التي تم إدعاءها.	The process of affirming that a claimed identity is correct by comparing the offered claims of identity with previously proven information stored in the identity card or PIV system. The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the PIV Card or system and associated with the identity being claimed.
Host-Based IDS ––	نظام اكتشاف الاختراقات المعتمد على المضيف	هي نظم اكتشاف الاختراقات التي تعمل على البيانات المُجمَّعة من داخل أحد أنظمة الحاسوب. تمنح تلك الأفضلية أنظمة اكتشاف الاختراقات المعتمدة على المضيف إمكانية أن تحدد بالضبط أي العمليات وأي حسابات المستخدمين التي تورطت في هجوم معين على نظام التشغيل بل وإنه على عكس أنظمة اكتشاف الاختراقات المعتمدة على الشبكة فان تلك الأنظمة تستطيع اكتشاف النتيجة المقصودة من محاولة هجوم معينة لأنها تستطيع الوصول مباشرة ومراقبة ملفات البيانات وعمليات النظام التي عادة ما يتم استهدافها في الهجمات.	IDSs which operate on information collected from within an individual computer system. This vantage point allows host-based IDSs to determine exactly which processes and user accounts are involved in a particular attack on the Operating System. Furthermore, unlike network-based IDSs, host-based IDSs can more readily “see” the intended outcome of an attempted attack, because they can directly access and monitor the data files and system processes usually targeted by attacks.
Network-Based IDS ––	نظام اكتشاف الاختراقات المعتمد على الشبكة	أنظمة اكتشاف الاختراقات التي تتبع الهجمات من خلال التقاط وتحليل حزم البيانات الموجودة في الشبكة. بالاستماع إلى الإشارات داخل الشبكة أو المُبَدِل يستطيع نظام اكتشاف الاختراقات المعتمد على الشبكة مراقبة تدفق البيانات الذي يؤثر في العديد من أجهزة المضيف المرتبطة بإشارة الشبكة.	IDSs which detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment.
Image –	صورة	نسخة مُحكمة (طبق الأصل) لكل البيانات الالكترونية الموجودة على أحد الأجهزة. يتم عمل تلك النسخة بطريقة تضمن عدم تغير المعلومات.	An exact bit-stream copy of all electronic data on a device, performed in a manner that ensures the information is not altered.
Impact –	تأثير	حجم الضرر المتوقع أن ينتُج من تداعيات الإفصاح عن البيانات أو تغييرها أو تدميرها دون تصريح أو فقد المعلومات وانقطاع استمرارية توفر نظام المعلومات.	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.
Inappropriate Usage –	سوء الاستخدام	شخص ينتهك سياسات استخدام الحاسوب المقبولة.	A person who violates acceptable computing use policies.
Incident –	حادثة	انتهاك أو تهديد خطير بانتهاك السياسات الأمنية للحاسوب أو سياسات الاستخدام المتفق عليها أو الممارسات القياسية لأمن الحاسوب. حادثة قد تعرض بالفعل أو تجعل من المحتمل تعرض سرية نظام معلومات أو تكامله أو استمرارية توفر خدمته أو عملياته أو مخازن بياناته للخطر أو قد تنقل أو تُشكِّل انتهاكاً أو تهديداً خطيراً لسياسته الأمنية أو إجراءاته الأمنية أو سياسات استخدامه المقبولة.	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

The mitigation of violations of security policies and recommended practices.	التخفيف من انتهاكات السياسات الأمنية والتعريف بالممارسات المُوصى بها.	معالجة الحوادث	Incident Handling –
The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's IT systems(s).	توثيق مجموعة من التعليمات والإجراءات المُعَدِّة سلفاً لاكتشاف ومعالجة والحد من تداعيات الهجمات الالكترونية الخبيثة ضد أنظمة تقنية المعلومات الخاصة بأحد المنظمات.	خطة معالجة الحوادث	Incident Response Plan –
Evidence that tends to increase the likelihood of fault or guilt.	دليل يميل إلى زيادة احتمالية الخطأ أو الذنب.	دليل إدانة	Inculpatory Evidence –
A sign that an incident may have occurred or may be currently occurring.	علامة على احتمالية وقوع حادثة أو وقوعها بالفعل في تلك الأثناء.	مؤشر الحادثة	Indication –
An instance of an information type.	نموذج من أحد أنواع المعلومات.	معلومة	Information –
Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.	مقاييس لحماية المعلومات والدفاع عنها من خلال التأكد من استمرارية توفرها وتكاملها ومصداقيتها وسريتها وعدم إنكارها. تضم تلك المقاييس توفير إمكانية استعادة أنظمة المعلومات بدمج إمكانيات الحماية والتتبع والقدرة على رد الفعل.	تأمين المعلومات	Information Assurance –
Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.	موظف يمتلك السلطة القانونية أو التشغيلية لمعلومات محددة والمسئولية عن إنشاء عناصر التحكم الخاصة بإصدارها وتجميعها ومعالجتها ونشرها والتخلص منها.	مالك المعلومات	Information Owner –
Information and related resources, such as personnel, equipment, funds, and information technology.	المعلومات وما يتعلق بها من موارد مثل الكوادر البشرية والأجهزة والتمويل المالي وتقنية المعلومات	موارد المعلومات	Information Resources –
The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—	حماية المعلومات وأنظمتها من الوصول أو الاستخدام أو الإفصاح أو الخلل أو التغيير أو التدمير غير المُصرَّح به بهدف توفير سرية تلك المعلومات وتكاملها واستمرارية توفرها. حماية المعلومات وأنظمتها من الوصول أو الاستخدام أو الإعلان أو الخلل أو التغيير أو التدمير غير المصرَّح به لتوفير		
1) integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;	1) التكامل الذي يعنى الحماية ضد تغيير المعلومات وتدميرها كما يشمل أيضاً التأكد من مصداقية المعلومات وعدم إنكارها		
2) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and	2) السرية التي تعني استعمال قيود مرخصة للوصول إلى المعلومات والإعلان عنها بما في ذلك وسائل حماية الخصوصية وحق ملكية المعلومات		
3) availability, which means ensuring timely and reliable access to and use of information.	3) استمرارية توفر البيانات بمعنى التأكد من إتاحة الوصول للمعلومات واستخدمها في الحال وبشكل يُعتمد عليه.	أمن المعلومات	Information Security –
The requirements for information sharing by an IT system with one or more other IT systems or applications, for information sharing to support multiple internal or external organizations, missions, or public programs.	الحاجة إلى مشاركة المعلومات الموجودة في أحد أنظمة المعلومات مع نظام أخر أو عدة أنظمة أو تطبيقات أخرى بهدف تقديم الدعم لعدة منظمات أو مأموريات أو برامج عامة سواء كانت داخلية أو خارجية.	مشاركة المعلومات	Information Sharing –

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.	مجموعة من موارد المعلومات المنفصلة مُرتبة بغرض تجميع أو معالجة أو صيانة أو استخدام أو توزيع أو تنظيم المعلومات.	نظام معلومات	Information System –
Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.	موظف مسؤول عن كل عمليات إمدادات نظام المعلومات أو تطويره أو تكامله أو تغييره أو تشغيله أو صيانته.	مالك نظام المعلومات (أو مدير البرنامج)	Information System Owner (or Program Manager) –
Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for ensuring the appropriate operational security posture is maintained for an information system or program.	شخص أسند إليه رئيس مسؤولي أمن المعلومات داخل أحد الوكالات أو موظف إصدار التصريح أو موظف الإدارة أو مالك نظام المعلومات مسؤولية التأكد من صحة وضع التشغيل الأمني الخاص بأحد أنظمة المعلومات أو البرنامج.	موظف أمن نظام المعلومات	Information System Security Officer (ISSO) –
Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which—	أي جهاز أو نظام مرتبط أو نظام فرعي لجهاز معين تستخدمه وكالة تنفيذية في الحصول على المعلومات أو البيانات آلياً أو تخزينها أو معالجتها أو إدارتها أو تحريكها أو التحكم بها أو عرضها أو توجيهها أو تغييرها أو نقلها أو استقبالها. لتحقيق الأغراض السابقة يتم استخدام الأجهزة بواسطة الوكالة التنفيذية وسواء كان استخدام تلك الأجهزة مباشراً مقبل الوكالة التنفيذية أو بواسطة مقاول بموجب عقد ابرمه مع الوكالة التنفيذية يتطلب ذلك ما يلي		
1) requires the use of such equipment; or	1) إستخدام تلك الأجهزة		
2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.	2) أن يكون الاستخدام بأكبر قدر في أداء أحد الخدمات أو تزويد أحد المنتجات. يتضمن مصطلح تقنية المعلومات الحواسيب والأجهزة الملحقة والبرامج و برامج التشغيل المثبتة في ذاكرة القراءة والإجراءات المشابهة والخدمات (شاملةً خدمات الدعم) والموارد المتعلقة بذلك.	تقنية المعلومات	Information Technology –
A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization or in some instances, by a specific law, executive order, directive, policy, or regulation.	فئة محددة من المعلومات كأن تكون معلومات تتعلق بالخصوصية أو بالطب أو بالممتلكات أو بالنواحي المالية أو بالتحقيقات أو بالمقاول أو بإدارة الأمن. هذه المعلومات مُعرَّفة بواسطة إحدى المنظمات أو في بعض الأحيان بواسطة قانون معين أو قرار تنفيذي أو توجيه أو سياسة أو لائحة.	نوع المعلومات	Information Type –
Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.	مجموعة من التوجيهات واللوائح والقواعد والممارسات التي ترشد إلى كيفية قيام منظمة بإدارة وحماية وتوزيع المعلومات.	سياسة أمن المعلومات	Information Security Policy –
The process of blocking incoming packets that use obviously false IP addresses, such as reserved source addresses.	عملية رفض لحزم البيانات القادمة والتي يتضح استخدامها لعناوين وهمية لبروتوكول الانترنت مثل عناوين المصدر المحجوزة	تصفية حزم البيانات الواردة	Ingress Filtering –
A vector used in defining the starting point of an encryption process within a cryptographic algorithm.	متجه يُستخدَم في تحديد نقطة البداية لعملية تشفير في خوارزمية التشفير.	متجه بداية التشفير	Initialization Vector (IV) –
The entity that initiates an authentication exchange.	الكيان الذي يبدأ إحدى عمليات التصديق المتبادل.	محفِّز التصديق	Initiator –

An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.	كيان مُصرَّح له الوصول ولديه إمكانية إحداث الضرر بنظام المعلومات من خلال تدمير البيانات أو الإفصاح عنها أو تغييرها و/أو حجب الخدمة.	تهديد داخلي	Inside Threat –
Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.	الحماية ضد تغير المعلومات بشكل خاطئ أو تدميرها وكذلك التأكد من عدم إنكار البيانات والتأكد صحة التصديق. خاصية عدم تعرض البيانات الحساسة للتغيير أو الحذف بطريقة غير مُصرَّح بها ولا يمكن اكتشافها.	التكاملية	Integrity –
Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.	ما هو مفيد من معلومات أدبية وتقنية و/أو صناعية ومعرفة أو أفكار تبين الملكية وتتحكم في الاستخدام الملموس أو الافتراضي و/أو طريقة العرض.	الملكية الفكرية	Intellectual Property –
An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations.	أتفاق بين منظمتين تمتلكان أو تقومان على تشغيل أنظمة تقنية معلومات مترابطة بغرض توثيق المتطلبات التقنية لعملية الترابط. يدعم أتفاق الترابط الأمني أيضاً وجود مذكرة تفاهم أو مذكرة أتفاق بين المنظمتين.	أتفاق الترابط الأمني	Interconnection Security Agreement (ISA) –
A Certification Authority that is subordinate to another CA, and has a CA subordinate to itself.	هيئة توثيق تكون خاضعة لهيئة توثيق أخرى كما أنها ذاتها ينبثق عنها هيئة توثيق تابعة.	هيئة توثيق وسيطة	Intermediate Certification Authority (CA) –
In FIPS 201, interoperability allows any Government facility or information system, regardless of the cardholder's parent organization, to authenticate cardholder's identity using the credentials stored on the Personal Identity Verification (PIV) card.	في المادة رقم 201 من المعيار الفيدرالي لمعالجة البيانات بغض النظر عن هوية المنظمة التي ينتمي لها حامل البطاقة تسمح القدرة على العمل المشترك لأي منشأة حكومية أو نظام معلومات التحقق من هوية حامل البطاقة باستخدام عناصر اعتماد المصداقية المخزَّنة على بطاقة التعريف الشخصي.	القدرة على العمل المشترك	Interoperability –
Software that looks for suspicious activity and alerts administrators.	برنامج يقوم بالبحث عن الأنشطة المثيرة للريبة وتوجيه تنبيه لمديري النظام.	نظام اكتشاف الاختراقات	Intrusion Detection System (IDS) –
Systems which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.	أنظمة تستطيع اكتشاف الأنشطة التي تهدف لاختراق النظام وتستطيع أيضاً محاولة وقف تلك الأنشطة قبل الوصول لأهدافها.	أنظمة منع الاختراقات	Intrusion Prevention Systems –
Series of transformations that converts ciphertext to plaintext using the Cipher Key.	سلسلة من التحويلات التي تغير نص المُشَفَر إلى نص غير مُشفَّر باستخدام مفتاح ترميز.	الترميز المعكوس	Inverse Cipher –
An IP address is a unique number for a computer that is used to determine where messages transmitted on the Internet should be delivered. The IP address is analogous to a house number for ordinary postal mail.	هو رقم فريد غير قابل للتكرار يتم تخصيصه للحاسوب بغرض تحديد المكان الذي توجه إليه الرسائل المنقولة عبر الانترنت. عنوان بروتوكول الانترنت يشبه رقم المنزل الذي توجه إليه الرسائل في البريد العادي.	عنوان بروتوكول الانترنت	IP Address –

An Institute of Electrical and Electronic Engineers (IEEE) standard, Request For Comments (RFC) 2411, protocol that provides security capabilities at the Internet Protocol (IP) layer of communications. IPsec's key management protocol is used to negotiate the secret keys that protect Virtual Private Network (VPN) communications, and the level and type of security protections that will characterize the VPN. The most widely used key management protocol is the Internet Key Exchange (IKE) protocol.	أحد المعايير الصادرة عن معهد المهندسين الالكترونيين والكهربائيين تحت طلب التعليق رقم 2411 حيث يوفر ذلك البروتوكول إمكانيات الأمن لطبقة الاتصالات في بروتوكول الانترنت. يُستخدَم بروتوكول إدارة المفتاح الخاص بمعيار أمن بروتوكول الانترنت في التفاوض حول المفاتيح السرية التي تحمي الاتصالات عبر الشبكة الخاصة الافتراضية بالإضافة إلى تحديد مستوى ونوع الحماية الأمنية التي تميز الشبكة الخاصة الافتراضية. أكثر بروتوكولات إدارة المفاتيح انتشاراً هو بروتوكول تبادل مفاتيح الانترنت.	معيار أمن بروتوكول الانترنت IPsec	IP Security (IPsec) –
The net mission/business impact considering	التأثير الذي تحدثه الشبكة على الأعمال أو المهام فيما يخص	المخاطر المتعلقة بتقنية المعلومات	IT-Related Risk –
1) the likelihood that a particular threat source will exploit, or trigger, a particular information system vulnerability, and	1) احتمالية قيام أحد مصادر التهديد باستغلال أو استهداف الثغرات الأمنية في أحد أنظمة المعلومات .		
2) the resulting impact if this should occur. IT-related risks arise from legal liability or mission/business loss due to, but not limited to: Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information. Non-malicious errors and omissions. IT disruptions due to natural or man-made disasters. Failure to exercise due care and diligence in the implementation and operation of the IT.	2) التأثير الناتج إذا حدث ذلك. تنشأ مخاطر تقنية المعلومات من المسؤولية القانونية أو فقد المهام/الأعمال نتيجة لما يلي على سبيل المثال وليس الحصر: الإفصاح عن المعلومات أو تغييرها أو تدميرها دون تصريح سواء حدث ذلك نتيجة طريقة خبيثة أو غير خبيثة أو مصادفة الأخطاء وعملية الحذف غير الخبيثة . جوانب الخلل التي تصيب تقنية المعلومات نتيجة للكوارث الناتجة عن الطبيعة أو البشر الفشل في توفير الاهتمام والجهد المناسب لتطبيق وتشغيل أنظمة تقنية المعلومات		
A description of security principles and an overall approach for complying with the principles that drive the system design; i.e., guidelines on the placement and implementation of specific security services within various distributed computing environments.	وصف للمبادئ الأمنية والمفهوم العام للتماشي مع المبادئ التي توجه تصميم النظام بمعنى الإرشادات الخاصة بوضع وتطبيق خدمات أمنية معينة داخل أنواع متعددة من بيئات الحوسبة الموزعة.	هيكلية أمن تقنية المعلومات	IT Security Architecture –
The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.	الغرض من العروض التوعوية هو ببساطة تركيز الانتباه على الأمن حيث تسمح تلك العروض للأفراد بمعرفة شئون أمن تقنية المعلومات وبالتالي الاستجابة لتلك المعرفة.	الوعي بأمن تقنية المعلومات	IT Security Awareness –
Explains proper rules of behavior for the use of agency IT systems and information. The program communicates IT security policies and procedures that need to be followed.	يوضح ذلك البرنامج القواعد السلوكية السليمة لاستخدام الأنظمة التقنية والمعلومات الخاصة بأحد الوكالات. يشرح البرامج السياسات الأمنية والإجراءات الواجب إتباعها.	برنامج التدريب والتوعية بأمن تقنية المعلومات	IT Security Awareness and Training Program –
IT Security Education seeks to integrate all of the security skills and competencies of the various functional specialties into a common body of knowledge, adds a multidisciplinary study of concepts, issues, and principles (technological and social), and strives to produce IT security specialists and professionals capable of vision and pro-active response.	يهدف تعليم أمن تقنية المعلومات إلى ضم كل مهارات وقدرات الأمن من عدة تخصصات وظيفية داخل إطار عام من المعرفة بالإضافة إلى الدراسة متعددة الجوانب للمفاهيم والمسائل والمبادئ (التقنية والاجتماعية) كما يسعى ذلك التعليم لإخراج متخصصين ومحترفين في مجال الأمن يكون لديهم الرؤية والاستجابة السريعة.	تعليم أمن تقنية المعلومات	IT Security Education –
The five security goals are confidentiality, availability, integrity, accountability, and assurance.	الأهداف الخمسة للأمن هي السرية و استمرارية توفر الخدمة والتكاملية والمسؤولية والتأمين.	هدف أمن تقنية المعلومات	IT Security Goal –

An IT application or system that is solely devoted to security. For instance, intrusion detection systems (IDS) and public key infrastructure (PKI) are examples of IT security investments.	أحد تطبيقات أو أنظمة تقنية المعلومات المخصصة بالكامل للأمن. على سبيل المثال تعد أنظمة اكتشاف الاختراقات والبنية التحتية للمفتاح العام أمثلة للاستثمارات في أمن تقنية المعلومات.	استثمار في مجال أمن تقنية المعلومات	IT Security Investment –
Metrics based on IT security performance goals and objectives.	قياسات تعتمد على الأهداف والغايات من تنفيذ أمن تقنية المعلومات.	قياسات أمن تقنية المعلومات	IT Security Metrics –
The “documentation of IT security decisions” in an organization. NIST SP 800-12 categorizes IT Security Policy into three basic types:	توثيق لقرارات تقنية أمن المعلومات داخل أحد المنظمات. وقد صنفت المعهد الوطني للمقاييس و التقنية سياسات تقنية المعلومات إلى 3 أنواع أساسية:		
1) Program Policy—high-level policy used to create an organization’s IT security program, define its’ scope within the organization, assign implementation responsibilities, establish strategic direction, and assign resources for implementation.	1) سياسة برامج: نوع متقدم من السياسات الأمنية يُستخدم لإنشاء برنامج أمن تقنية المعلومات لأحدى المنظمات بالإضافة إلى تحديد نطاق أهدافها ومسئوليات التنفيذ واتجاهها الاستراتيجي والموارد المطلوبة للتنفيذ.		
2) Issue-Specific Policies—address specific issues of concern to the organization, such as contingency planning, the use of a particular methodology for systems risk management, and implementation of new regulations or law. These policies are likely to require more frequent revision as changes in technology and related factors take place.	2) سياسات مخصصة لحالات معينة: تقوم بمعالجة مسائل معينة في المنظمة مثل التخطيط للحالات الطارئة واستخدام أسلوب معين في أنظمة إدارة المخاطر وتطبيق لوائح أو قانون جديد. قد تحتاج هذه السياسات إلى مراجعة متكررة مع حدوث التغيرات في مجال التقنية و ما يرتبط بذلك من عوامل.		
3) System-Specific Policies—address individual systems, such as establishing an access control list or in training users as to what system actions are permitted. These policies may vary from system to system within the same organization. In addition, policy may refer to entirely different matters, such as the specific managerial decisions setting an organization’s electronic mail (e-mail) policy or fax security policy.	3) سياسات مخصصة لأنظمة معينة: تعالج أنظمة منفردة مستقلة بذاتها مثل إنشاء قائمة تحكم في الوصول أو في تدريب المستخدمين على ما هو مسموح لهم من إجراءات النظام. هذه السياسات ربما تختلف من نظام لأخر داخل نفس المنظمة بالإضافة إلى أن السياسة ممكن أن تشير لأمور مختلفة تماماً مثل القرارات الإدارية الخاصة فيما يتعلق بإعداد البريد الالكتروني للمنظمة أو سياسة أمن الفاكسات بها.	سياسة أمن تقنية المعلومات	IT Security Policy –
IT Security Training strives to produce relevant and needed security skills and competencies by practitioners of functional specialties other than IT security (e.g., management, systems design and development, acquisition, auditing). The most significant difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus an individual’s attention on an issue or set of issues. The skills acquired during training are built upon the awareness foundation, in particular, upon the security basics and literacy material.	يسعى التدريب على أمن تقنية المعلومات إلى إخراج المهارات والكفاءات ذات الصلة والمطلوبة بواسطة ممارسي التخصصات الوظيفية فيما سوى أمن تقنية المعلومات (مثل الإدارة وتصميم النظم والتطوير والحصول على البيانات والتدقيق). أهم اختلاف بين التدريب والتوعية هو أن التدريب يسعى لتعليم المهارات التي تسمح للفرد بأداء وظيفة معينة بينما تهدف التوعية إلى تركيز انتباه الفرد على موضوع أو مجموعة موضوعات. المهارات المكتسبة أثناء التدريب تكون مبنية على أساس التوعية خصوصاً على أساسيات الأمن والمعرفة بالمواد.	التدريب على أمن تقنية المعلومات	IT Security Training –

A widely used authentication protocol developed at the Massachusetts Institute of Technology (MIT). In “classic” Kerberos, users share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to communicate with another user, Bob, authenticates to the KDC and is furnished a “ticket” by the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords, the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who capture the initial user-to-KDC exchange.	بروتوكول تصديق واسع الاستخدام تم تطويره داخل معهد مساتشوستيس للتقنية. في النسخة التقليدية لهذا البروتوكول يقوم المستخدمين بمشاركة كلمة مرور مع "مركز توزيع المفتاح" بمعنى أن المستخدم "X" الذي يرغب في التواصل مع المستخدم "Y" يحصل على تصديق من مركز توزيع المفتاح حيث يزوده المركز بـ "تذكرة" يستخدمها لإتمام التصديق مع المستخدم "Y" وعليه فان اعتماد التصديق في بروتوكول Kerberos على كلمات المرور يجعله عرضه لهجمات "القاموس" التي تتم دون الاتصال بالشبكة من قِبَل المتصنتين الذين يلتقطون الاتصال المبدئي بين المستخدم ومركز توزيع المفتاح.	بروتوكول التصديق الشبكي Kerberos	Kerberos –
A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification.	قيمة تستخدم للتحكم في عمليات تشفيرية مثل فك التشفير أو التشفير أو إصدار التوقيع أو التحقق من صحة التوقيع.	مفتاح	Key –
The three cryptographic keys (Key1, Key2, Key3) that are used with a Triple Data Encryption Algorithm mode.	مفاتيح التشفير الثلاثة (Key1, Key2, Key3) التي تُستخدم في وضعية خوارزمية تشفير بيانات ثلاثية	حزمة ثلاثية للمفاتيح	Key Bundle –
A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. The processes of managing (e.g., generating, storing, transferring, auditing) the two components of a cryptographic key by two key component holders.	إيداع المفتاح الخاص لأحد المشتركين وما يتعلق به من معلومات أخرى طبقاً لاتفاق تأمين أو عقد مشابه ملزم للمشترك حيث تقضى شروطه احتفاظ أحد الوكلاء أو أكثر من وكيل بالمفتاح الخاص للمشترك مقابل منفعة للمشترك أو لصاحب العمل أو أطراف أخرى طبقاً للشروط المحددة سلفاً في الاتفاق. العمليات الخاصة بإدارة (إصدار ، تخزين ، نقل ، تدقيق) اثنين من مكونات أحد مفاتيح التشفير بواسطة اثنين من مالكي مكونات المفتاح.	ضمان تواجد المفتاح / تأمين المفتاح	Key Escrow –
A system that entrusts the two components comprising a cryptographic key (e.g., a device unique key) to two key component holders (also called "escrow agents").	نظام يعهد باثنين من المكونات التي تضم مفتاح تشفير (المفتاح الفريد لأحد الأجهزة مثلاً) لاثنين من مالكي مكونات المفتاح (يطلق عليهم "وكلاء الضمان" أيضاً) .	نظام ضمان تواجد المفتاح / نظام تأمين المفتاح	Key Escrow System –
The process by which cryptographic keys are securely distributed among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods (consists of key transport plus key agreement).	عملية يتم بواسطتها توزيع مفاتيح التشفير بأمان بين وحدات التشفير النمطية باستخدام أساليب نقل يدوية (مثل محمِّلات المفاتيح) وأساليب آلية (مثل برتوكولات نقل المفتاح و/أو اتفاق المفتاح) أو مزيج من الأساليب الآلية واليدوية (تتكون من نقل مفتاح بالإضافة إلى اتفاق مفتاح) .	إنشاء مفتاح	Key Establishment –
The process of exchanging public keys in order to establish secure communications.	عملية تبادل المفاتيح العامة بغرض إقامة اتصالات آمنة.	تبادل المفاتيح	Key Exchange –
Routine used to generate a series of Round Keys from the Cipher Key.	أحد الدوال البرمجية التي تُستخدَم في إصدار سلسلة من المفاتيح المتعاقبة من مفتاح الترميز.	توسيع المفتاح	Key Expansion –
Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.	أرقام عشوائية أو أرقام شبه عشوائية ومعايير تشفير تُستخدَم في إصدار مفاتيح التشفير.	مكونات إصدار المفتاح	Key Generation Material –

A self-contained unit that is capable of storing at least one plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module.	وحدة مستقلة قادرة على تخزين نص غير مُشفَّر واحد على الأقل أو أحد مفاتيح التشفير المُشفَّرة أو أحد مكونات المفتاح بحيث يمكن نقلها إلى أحد وحدات التشفير النمطية عند طلبها.	مُحمِّل المفاتيح	Key Loader –
The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.	هي تلك الأنشطة التي تتطلب معالجة مفاتيح التشفير وما يتعلق بها من معايير أمن أخرى (مثل متجهات بداية التشفير وكلمات المرور) أثناء الدورة الكاملة للمفاتيح شاملة إصدارها وتخزينها وإنشاءها وإدخالها وإخراجها وتحويلها للقيمة الصفرية.	إدارة المفاتيح	Key Management –
Two mathematically related keys having the properties that	زوج من المفاتيح المرتبطة حسابياً يتميزان بالخواص التالية		
(1) one key can be used to encrypt a message that can only be decrypted using the other key, and	1) أحد المفتاحين يمكن استخدامه في تشفير أحد الرسائل التي لا يمكن فك تشفيرها إلا بواسطة المفتاح الأخر		
(2) even knowing one key, it is computationally infeasible to discover the other key. A public key and its corresponding private key; a key pair is used with a public key algorithm.	2) حتى في حالة معرفة أحد المفاتيح يظل اكتشاف المفتاح الأخر غير قابل للتنفيذ رياضياً. أحد المفاتيح العامة وما يتفق معه من المفاتيح الخاصة يمثلان زوج من المفاتيح ذات خوارزمية مفتاح عام.	زوج مفاتيح	Key Pair –
The secure transport of cryptographic keys from one cryptographic module to another module.	النقل الآمن لمفاتيح التشفير من وحدة تشفير نمطية إلى وحدة أخرى.	نقل المفاتيح	Key Transport –
A method of encrypting keys (along with associated integrity information) that provides both confidentiality and integrity protection using a symmetric key algorithm.	أحد أساليب تشفير المفاتيح (و معلومات التكاملية ذات الصلة) التي توفر حماية السرية والتكاملية باستخدام خوارزمية مفتاح متناظر.	لفّ المفاتيح	Key Wrap –
A message authentication code that uses a cryptographic key in conjunction with a hash function.	شفرة تصديق للرسالة تستخدم مفتاح تشفير مرتبط بدالة اختزال.	شفرة تصديق الرسالة المعتمدة على الاختزال المُشَفَّر	Keyed-hash based message authentication code (HMAC) –
The process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails.	تُستخدَم هذه العملية لعرض أو تسجيل كلاً من ضربات لوحة المفاتيح التي يقوم بها مستخدم الحاسوب و الردود التي ترد للحاسوب أثناء الجلسات التفاعلية في التعامل مع الشبكة. تعد مراقبة الكتابة على لوحة المفاتيح من الحالات الخاصة في سجل التتبع.	مراقبة الكتابة على لوحة المفاتيح	Keystroke Monitoring –
The security objective of granting users only those accesses they need to perform their official duties.	الهدف الأمني من منح المستخدمين صلاحيات الوصول التي يحتاجونها لتنفيذ مسؤولياتهم الرسمية فقط.	الحد الأدنى من الامتيازات	Least Privilege –
Link encryption encrypts all of the data along a communications path (e.g., a satellite link, telephone circuit, or T1 line). Since link encryption also encrypts routing data, communications nodes need to decrypt the data to continue routing.	يقوم تشفير الرابط بتشفير جميع البيانات في قناة الاتصال (على سبيل المثال رابط قمر اصطناعي أو دائرة تليفونية أو خط T1) وحيث أن تشفير الرابط يقوم أيضاً بتشفير بيانات التوجيه فإن نقاط الاتصال تحتاج فك تشفير المعلومات لتستمر عملية التوجيه	تشفير قناة الاتصال	Link Encryption –
A Registration Authority with responsibility for a local community.	هيئة تسجيل تضطلع بالمسئولية تجاه المجتمع المحلي.	هيئة تسجيل محلية	Local Registration Authority (LRA) –
An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact of low.	نظام معلومات تكون فيه أهداف الأمن الثلاثة (السرية والتكاملية استمرارية توفر الخدمة) حاصلة على درجة "منخفض" في التأثير المحتمل طبقاً للمعيار الفيدرالي لمعالجة البيانات رقم FIPS 199.	نظام منخفض التأثير	Low Impact System –

A virus that attaches itself to documents and uses the macro programming capabilities of the document's application to execute and propagate.	فيروس يلصق نفسه بالمستندات ثم يستخدم إمكانية الماكرو البرمجية الخاصة بأحد تطبيقات المستند لتشغيل ونشر نفسه.	فيروس الماكرو	Macro Virus –
An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.	أحد التطبيقات التي تتطلب عناية خاصة بالجوانب الأمنية نظراً لخطورة و أهمية الضرر الناتج عن فقد المعلومات من ذلك التطبيق أو سوء استخدامها أو الوصول لها دون تصريح أو تغييرها. ملحوظة: كل التطبيقات الحكومية تتطلب حد معين من مستويات الأمن إلا أن هناك تطبيقات محددة – بسبب ما تحويه من معلومات – تتطلب إشراف إداري خاص ويجب التعامل معها كتطبيق رئيسي. ويجب إعطاء أمن كافي للتطبيقات الأخرى من خلال أمن الأنظمة التي تشغلها	تطبيق رئيسي	Major Application –
An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.	أحد أنظمة المعلومات التي تتطلب عناية خاصة في إدارتها نظراً لما تمثله من أهمية لرسالة الوكالة أو نظراً للتكاليف العالية لتطويرها أو تشغيلها أو صيانتها أو نظراً لدورها المهم في إدارة البرامج أو النواحي المالية أو الممتلكات أو غيرها من موارد الوكالة .	نظام معلومات رئيسي	Major Information System –
Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host.	أحد البرامج أو برامج التشغيل المثبتة في ذاكرة القراءة والتي تقوم بتنفيذ عملية غير مصرَّح بها فتُحدِث تأثيراً مضاداً على السرية أو التكاملية أو استمرارية توفر نظام معلومات. أحد البرمجيات الخبيثة التي تصيب جهاز المضيف مثل الفيروس أو الدودة أو حصان طروادة أو غيرها من كيانات المعتمدة على الشفرة.	الشفرة الخبيثة	Malicious Code –
A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.	برنامج يتم إدخاله إلى أحد الأنظمة - عادة ما يتم ذلك خفية - لانتهاك نواحي السرية والتكاملية واستمرارية توفر الخدمة الخاصة ببيانات الضحية أو تطبيقاته أو نظام التشغيل الخاص به أو مضايقة الضحية أو إحداث خلل لديه.	البرمجيات الضارة	Malware –
An attack on the authentication protocol run in which the attacker positions himself in between the claimant and verifier so that he can intercept and alter data traveling between them.	هجوم يستهدف عمل بروتوكول التصديق حيث يقوم المهاجم بوضع نفسه بين المتقدم بطلب التوثيق والطرف المسؤول عن التحقق من الهوية حتى يتمكن من اعتراض وتغيير البيانات المنقولة بينهما.	الهجوم على برتوكول التوثيق باعتراض البيانات	Man-in-the-middle Attack (MitM) –
The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.	عناصر التحكم الأمنية مثل إجراءات الوقاية وعوامل المقاومة الخاصة بأحد أنظمة المعلومات والتي تُركِّز على إدارة المخاطر وإدارة النواحي الأمنية المتعلقة بذلك النظام.	إدارة عناصر التحكم	Management Controls –
A means of restricting access to system resources based on the sensitivity (as represented by a label) of the information contained in the system resource and the formal authorization (i.e., clearance) of users to access information of such sensitivity. Access controls (which) are driven by the results of a comparison between the user's trust level or clearance and the sensitivity designation of the information.	وسيلة تحديد للوصول إلى موارد النظام بناءاً على حساسية المعلومات (ممثلةً بملصق) الموجودة داخل موارد النظام والتصريح الرسمي (الترخيص مثلاً) للمستخدمين بالوصول إلى المعلومات التي لها ذلك القدر من الحساسية. عناصر التحكم التي تُشتَق نتيجة للمقارنة بين مستوى الثقة في المستخدم أو التصريح الممنوح له وحساسية المعلومات.	التحكم الإجباري في الوصول	Mandatory Access Control –

The format and information required to be displayed on a PIV card. Also known as the Standard Topography.	النسق والمعلومات المطلوب عرضها على بطاقة التعريف الشخصي. ويطلق عليها أيضاً بيانات التعريف الأساسية.	بيانات التعريف الإجبارية	Mandatory Topography –
A non-electronic means of transporting cryptographic keys by physically moving a device, document or person containing or possessing the key or a key component. A non-electronic means of transporting cryptographic keys.	وسيلة غير آلية لنقل مفاتيح التشفير من خلال التحريك المادي لجهاز أو مستند أو شخص يحمل أو يمتلك المفتاح أو أحد مكوناته. وسيلة غير إلكترونية لنقل مفاتيح التشفير	النقل اليدوي للمفاتيح	Manual Key Transport –
When an unauthorized agent claims the identity of another agent it is said to be masquerading.	عندما يقوم عميل غير مصرَّح له بادعاء الهوية الخاصة بعميل أخر يطلق على ذلك انتحال هوية أو تنكر.	انتحال الهوية / التنكر	Masquerading –
The process of comparing biometric information against a previously stored template(s) and scoring the level of similarity.	مقارنة معلومات المقاييس الحيوية مع نموذج معد سلفاً وتسجيل مستوى التشابه.	تطابق / مطابقة	Match/matching –
Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, LSI memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.	الوسائل التي تُسجَل عليها المعلومات أو تُخزَّن أو تُطبَع داخل أحد أنظمة المعلومات مثل الأدوات المادية وأسطح الكتابة التي تشمل على سبيل المثال وليس الحصر الأشرطة الممغنطة والأقراص الضوئية والأقراص الممغنطة وشرائح الذاكرة ذات التكامل واسع النطاق والمطبوعات (لكنها لا تضم وسائل العرض).	وسائل نقل البيانات	Media –
A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.	مصطلح عام يُطلَق على الإجراءات التي يتم اتخاذها لجعل البيانات - المكتوبة على أحد الوسائل - غير قابلة للاسترجاع سواء بواسطة الأدوات المعتادة أو غير المعتادة.	تطهير البيانات	Media Sanitization –
A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection.	مستند تم إعداده بين طرفين أو أكثر لتحديد ما يخصهم من مسؤوليات في إنجاز هدف معين أو مهمة معينة. في هذا الدليل تحدد "مذكرة التفاهم/ مذكرة الاتفاق" المسؤوليات الملقاة على طرفين أو أكثر من المنظمات في إقامة وتشغيل وتأمين الوصلات البينية للنظام.	مذكرة تفاهم / مذكرة اتفاق	Memorandum of Understanding/Agreement (MOU/A) –
A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.	معادلة تشفير يتم تطبيقها على البيانات حيث تستخدم مفتاح متناظر لاكتشاف ما تشهده البيانات من تغيير مقصود أو غير مقصود	شفرة التصديق الخاصة بالرسالة	Message Authentication Code (MAC) –
A cryptographic checksum, typically generated for a file that can be used to detect changes to the file; Secure Hash Algorithm-1 (SHA-1) is an example of a message digest algorithm	معادلة تشفير يتم استحداثها بشكل نموذجي لأحد الملفات لكي تُستخدَم في اكتشاف ما حدث من تغييرات للملف. تعد خوارزمية الاختزال الآمنة مثالاً لخوارزمية موجز الرسالة.	موجز الرسالة	Message Digest –
Tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.	أدوات مصممَة لتسهيل اتخاذ القرارات وتحسين الأداء والمسؤولية من خلال تجميع وتحلل وإصدار التقارير عن البيانات المتعلقة بالأداء.	قياسات	Metrics –
A measure of the difficulty that an attacker has to guess the most commonly chosen password used in a system.	مقياس الصعوبة التي يواجهها المهاجم لتخمين كلمة المرور المختارة الأكثر شيوعاً والمستخدمة في نظام.	معامل صعوبة تخمين كلمة المرور	Min-Entropy –

An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system.	أحد التطبيقات - ولكنه ليس تطبيقاً رئيسياً - يتطلب عناية بجوانب الأمن فيه نظراً لخطورة وأهمية الضرر الناتج عن فقد المعلومات منه أو سوء استخدامها أو الوصول لها دون تصريح أو تغييرها. تكون التطبيقات الثانوية بشكل نموذجي جزء من نظام الدعم العام.	تطبيق ثانوي	Minor Application –
A technique used to disguise a file's content by changing the file's name to something innocuous or altering its extension to a different type of file, forcing the examiner to identify the files by file signature versus file extension.	أسلوب يُستخدَم في إخفاء محتوى أحد الملفات بواسطة تغيير اسم الملف إلى شيء غير ضار أو تغيير امتداده بامتداد نوع أخر من الملفات مما يرغم المسؤول عن الفحص تحديد نوع الملف بمقارنة توقيع الملف مع امتداده.	التسمية المغلوطة للملفات	Misnamed Files –
Any telecommunications or information system that is defined as a national security system (Federal Information Security Management Act of 2002 - FISMA) or processes any information the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency.	أي نظام للاتصالات أو المعلومات يُعرَّف بأن له طابع أمن قومي (حسب القانون الفيدرالي لإدارة أمن المعلومات لعام FISMA 2002) أو ذلك النظام الذي يعالج معلومات يُحدِث فقدها أو سوء استخدامها أو كشفها أو الوصول غير المُصرَّح لها تأثيراً موهِناً على مهمة وكالة معينة.	نظام ذو مهام حرجة	Mission Critical –
Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.	برامج أو أجزاء من برامج تُحصَّل من أنظمة معلومات بعيدة وتُنقل عبر شبكة وتُنفَذ على أحد أنظمة المعلومات المحلية دون الحاجة إلى قيام المستقبِل بتثبيتها أو تنفيذها.	الشفرة المتنقلة	Mobile Code –
Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript).	تقنيات برمجية توفر آليات لإنتاج واستخدام الشفرة المتنقلة (مثل الجافا والجافا سكريبت وأكتف إكس X وفى بى سكريبت) .	تقنيات الشفرة المتنقلة	Mobile Code Technologies –
A self-contained, transportable shell custom-fitted with the specific IT equipment and telecommunications necessary to provide full recovery capabilities upon notice of a significant disruption.	موقع صغير مستقل قابل للنقل ومُجَهَز بأجهزة تقنية المعلومات والاتصالات الضرورية لتوفير إمكانيات الاسترجاع الكامل للبيانات بمجرد استشعار وجود خلل خطير.	الموقع المتنقل	Mobile Site –
Programs that are goal-directed and capable of suspending their execution on one platform and moving to another platform where they resume execution.	برامج محددة الهدف لها القدرة على إيقاف تنفيذ نفسها على أحد المنصات والانتقال إلى منصة أخرى حيث يمكنها استكمال عملية التنفيذ.	عميل البرنامج المتنقل	Mobile Software Agent –
An algorithm for the cryptographic transformation of data that features a symmetric key block cipher algorithm.	خوارزمية للنقل المُشفَّر للبيانات تشبه خوارزمية تشفير قالب ذات مفتاح متناظر.	وضعية التشغيل	Mode of Operation –
An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high.	نظام معلومات يكون فيه أحد أهداف الأمن (السرية والتكاملية واستمرارية توفر الخدمة) ذو قيمة "متوسطة" في التأثير المحتمل طبقاً للمعيار الفيدرالي لمعالجة البيانات رقم FIPS 199 مع عدم حصول التأثير المحتمل لأي من الأهداف الأخرى على قيمة "مرتفعة".	نظام معتدل التأثير	Moderate Impact System –
The security risks resulting from a mobile software agent visiting several platforms.	المخاطر الأمنية الناتجة عن أحد عملاء البرامج المتنقلة الذي يتحرك بين عدة منصات.	مشكلة متنقلة	Multi-Hop Problem –

A single incident that encompasses two or more incidents.	حادثة مفردة تضم في جنباتها حادثتين أو أكثر.	حادثة متعددة الجوانب	Multiple Component Incident –
An extensible mechanism for email. A variety of MIME types exist for sending content such as audio using the Simple Mail Transfer Protocol (SMTP) protocol.	آلية للبريد الالكتروني قابلة للتمديد. يوجد أنواع متعددة من امتدادات بريد الانترنت متعددة الأغراض لإرسال المحتوى مثل الملفات الصوتية باستخدام برتوكول نقل البريد البسيط.	امتدادات بريد الانترنت متعددة الأغراض	Multipurpose Internet Mail Extensions (MIME) –
It occurs when parties at both ends of a communication activity authenticate each other.	يحدث التصديق المتبادل عند قيام الأطراف الموجودة على نهايتي قناة الاتصال بالتصديق على بعضهما البعض.	التصديق المتبادل	Mutual Authentication –
An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.	كيان تنظيمي مسؤول عن تحديد أسماء مُميِّزة والتأكد من أن كل اسم مُميِّز له معنى وفريد لم يتكرر داخل حدود نطاقه.	هيئة التسمية	Naming Authority –
Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States.	خدمات الاتصالات المُستخدمة في الحفاظ على حالة من الاستعداد أو الاستجابة والقدرة على إدارة أي حدث أو أزمة (محلية أو قومية أو عالمية) تُسبّب أو قد تُسبِب إصابات أو ضرر للسكان أو تدمير أو فقد للممتلكات أو تزعزع أو تهدد الأمن القومي أو قدرة الدولة على الاستعداد للطوارئ.	خدمات الاتصالات الخاصة بقدرة الأمن القومي على الاستعداد للطوارئ	National Security Emergency Preparedness Telecommunications Services –
A process that can be used to determine an organization’s awareness and training needs. The results of a needs assessment can provide justification to convince management to allocate adequate resources to meet the identified awareness and training needs.	عملية يمكن استخدامها لتحديد احتياجات إحدى المنظمات من التوعية والتدريب. من الممكن اتخاذ نتائج تلك العملية كمبرر لإقناع الإدارة بتخصيص موارد كافية لتلبية ما تم تشخيصه من احتياجات التوعية والتدريب.	تقدير الاحتياجات (التوعية والتدريب في مجال أمن المعلومات)	Needs Assessment (IT Security Awareness and Training) –
A U.S. Government initiative originated to meet the security testing needs of both information technology (IT) consumers and producers. NIAP is a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) in fulfilling their respective responsibilities under Public Law (PL) 100-235 (Computer Security Act of 1987). The partnership combines the extensive IT security experience of both agencies to promote the development of technically sound security requirements for IT products and systems and appropriate measures for evaluating those products and systems.	مبادرة تقدمت بها الحكومة الأمريكية لتلبية احتياجات الاختبار الأمني لدى كلاً من مستهلكي ومنتجي تقنية المعلومات. تعد تلك المبادرة ثمرة التعاون بين المعهد الوطني للمقاييس والتقنية من جهة ووكالة الأمن القومي من جهة أخرى حيث يسعون للوفاء بمسؤولياتهم المحددة في القانون العام رقم 235-100 (قانون أمن الحاسوب سنة 1987). تلك الشراكة توحد بين الخبرة الواسعة لكلتا الوكالتين في مجال أمن تقنية المعلومات لتشجيع تطوير ما هو صحيح تقنياً من المتطلبات الأمنية للمنتجات والأنظمة والمقاييس المناسبة لتقييم هذه المنتجات والأنظمة.	الشراكة القومية لتأمين المعلومات	National Information Assurance Partnership (NIAP) –

Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. It is the security service by which the entities involved in a communication cannot deny having participated. Specifically the sending entity cannot deny having sent a message (non-repudiation with proof of origin) and the receiving entity cannot deny having received a message (non-repudiation with proof of delivery).	تأكيد على أن مُرسِل المعلومات حاصل على إثبات لتسليمها وأن متلقي تلك المعلومات قد ورد له إثبات لهوية المُرسِل بحيث لا يستطيع أحدهما إنكار قيامه بمعالجة المعلومات. هي الخدمة الأمنية التي بها لا تستطيع الكيانات المشاركة فيها أحد عمليات الاتصال إنكار تلك المشاركة وبشكل أكثر تفصيلاً فان الكيان المُرسِل لا يستطيع إنكار قيامه بإرسال رسالة (دليل عدم إنكار المصدر) والكيان المستقبل لا يستطيع إنكار تسلمُه لتلك الرسالة (دليل عدم إنكار التسليم) .	عدم الإنكار	Non-repudiation –
A value used in security protocols that is never repeated with the same key. For example, challenges used in challenge-response authentication protocols generally must not be repeated until authentication keys are changed, or there is a possibility of a replay attack. Using a nonce as a challenge is a different requirement than a random challenge, because a nonce is not necessarily unpredictable.	هي قيمة تُستخدَم في برتوكولات الأمن ولا يمكن تكرارها مطلقاً في نفس المفتاح. على سبيل المثال الأسئلة المُستخدَمة في ببروتوكولات التصديق التي تعتمد على "سؤال وإجابة" لتحديد الهوية يجب أن تكون عموماً غير مكررة حتى يتم تغيير مفتاح التصديق أو وجود احتمالية هجوم إعادة الإرسال. استخدام تلك القيمة غير القابلة للتكرار كسؤال يعد مطلب مختلف عن السؤال العشوائي لأن تلك القيمة ليست بالضرورة غير قابلة للتخمين.	قيمة غير قابلة للتكرار	Nonce –
A passive entity that contains or receives information.	كيان غير نشط يحتوى أو يستقبل معلومات.	كائن	Object –
A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the four policies and cryptographic algorithms supported.	رقم ذو نسق خاص يتم تسجيله في منظمة للمقاييس تتمتع بشهرة دولية. المُعرِّف الفريد المكوّن من حروف هجائية و/أو أرقام يتم تسجيله في المنظمة الدولية للقياسات "أيزو" بغرض الإشارة إلى كائن أو إلى صنف معين يستخدمان لتمييز كل من سياسات وخوارزميات التشفير الأربعة المدعومة في البنية التحتية للمفاتيح العامة للحكومة الفيدرالية.	مُعرِّف الكائن	Object Identifier –
Refers to data that is not stored within the PIV card or computation that is not done by the Integrated Circuit Chip (ICC) of the PIV card.	تشير إلى البيانات غير المخزّنة على بطاقة التعريف الشخصية أو تلك العملية الحسابية التي لم تُنفذ بواسطة شريحة الدائرة المتكاملة في بطاقة التعريف الشخصي.	بطاقة بيانات غير مخزنة	Off-Card –
An attack where the attacker obtains some data (typically by eavesdropping on an authentication protocol run, or by penetrating a system and stealing security files) that he/she is able to analyze in a system of his/her own choosing.	هجوم يحصل فيه المهاجم على بعض البيانات (من خلال التصنت على عمل برتوكول التصديق أو اختراق أحد الأنظمة وسرقة بعض الملفات الأمنية) التي يكون قادراً على تحليلها مستخدماً نظام من اختياره.	الهجوم بدون الاتصال	Off-line Attack –
Refers to data that is stored within the PIV card or computation that is done by the ICC of the PIV card.	تشير إلى البيانات مخزّنة على بطاقة التعريف الشخصية أو تلك العملية الحسابية المنفذة بواسطة شريحة الدائرة المتكاملة في بطاقة التعريف الشخصي.	بطاقة بيانات مخزنة	On-Card –
An attack against an authentication protocol where the attacker either assumes the role of a claimant with a genuine verifier or actively alters the authentication channel. The goal of the attack may be to gain authenticated access or learn authentication secrets.	هجوم على بروتوكول التصديق ينتحل فيه المهاجم صفة مقدم طلب أمام المسئول عن التحقق من الهوية أو يقوم بتغير قناة التصديق بطريقة نشطة. قد يكون الهدف من ذلك الحصول على الوصول المصدق عليه أو معرفة أسرار التصديق.	هجوم مباشر	On-line Attack –

An on-line protocol used to determine the status of a public key certificate.	بروتوكول للاتصال المباشر يُستخدَم لتحديد حالة أحد شهادة مفتاح عام.	بروتوكول تحديد حالة الشهادة بالاتصال المباشر	On-Line Certificate Status Protocol (OCSP) –
Hash algorithms which map arbitrarily long inputs into a fixed-size output such that it is very difficult (computationally infeasible) to find two different hash inputs that produce the same output. Such algorithms are an essential part of the process of producing fixed-size digital signatures that can both authenticate the signer and provide for data integrity checking (detection of input modification after signature).	تقوم خوارزميات اختزال بتحويل المدخلات الطويلة إلى مخرجات محدد الحجم بحيث يكون من الصعوبة (غير ممكن حسابياً) إيجاد زوج من مدخلات الاختزال ينتجان نفس المُخرَج. هذه الخوارزمية تعد جزءاً أساسياً في عملية إنتاج توقيعات رقمية محددة الحجم لها إمكانية التصديق على هوية من قام بالتوقيع والتحقق من تكاملية البيانات (اكتشاف تغيير المدخلات بعد التوقيع) .	خوارزمية الاختزال ذات الاتجاه الواحد	One-Way Hash Algorithm –
An on-line protocol used to determine the status of a public key certificate.	بروتوكول للاتصال المباشر يُستخدَم لتحديد حالة شهادة مفتاح عام.	بروتوكول تحديد حالة الشهادة بالاتصال المباشر	Online Certification Status Protocol (OCSP) –
The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).	عناصر أمنية (الإجراءات الوقائية وعوامل المقاومة) لنظام معلومات يجري تنفيذها وتطبيقها بواسطة البشر (مقارنة بتلك التي تُطبقها الأنظمة) .	عناصر التحكم في التشغيل	Operational Controls –
A Personal Identity Verification (PIV) card having both the Standard Topography (Mandatory Topography) features and the Optional features as defined in FIPS 201 sections 4.1.4.3 and 4.1.4.4.	بطاقة تعريف شخصية لها مميزات بيانات التعريف الأساسية (الإجبارية) وكذلك المميزات الاختيارية المنصوص عليها في البنود رقم 4.1.4.3 و4.1.4.4 من المعيار الفيدرالي لمعالجة البيانات رقم 201 .	بيانات التعريف الاختيارية	Optional Topography –
An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.	كيان غير مُصرَّح له الوصول من خارج النطاق ولديه إمكانية إحداث الضرر بنظام معلومات من خلال تدمير البيانات أو الإفصاح عنها أو تغييرها أو حجب الخدمة.	تهديد خارجي	Outside Threat –
Software that observes and records network traffic.	برنامج يقوم بملاحظة وتسجيل حركة التدفق عبر الشبكة.	ملتقط حزم البيانات	Packet Sniffer –
The organization that is applying for the Personal Identity Verification card on behalf of an applicant. Typically this is an organization for whom the applicant is working.	المنظمة التي تتقدم للحصول على بطاقة التعريف الشخصي بدلاً من مقدم الطلب. وعادة ما تكون هي المنظمة التي يعمل لديها مقدم الطلب.	المنظمة العليا	Parent Organization –
An attack against an authentication protocol where the attacker intercepts data traveling along the network between the claimant and verifier, but does not alter the data (i.e. eavesdropping).	هجوم على بروتوكول التصديق يعترض فيه المهاجم البيانات المتدفقة عبر الشبكة بين مقدم الطلب وجهة التصديق على الهوية ولكن دون تغيير البيانات (بمعنى أنه تَنَصُت).	مهاجم غير نشط	Passive Attack –
A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. A protected character string used to authenticate the identity of a computer system user or to authorize access to system resources. A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.	سر يحتفظ به مقدم الطلب في ذاكرته ويستخدمه للتصديق على هويته. عادة ما تكون كلمات المرور على شكل سلاسل حرفية و/أو رقمية. هي سلسلة حرفية محمية تُستخدَم في التصديق على هوية مستخدم نظام حاسوب أو التصريح بالوصول إلى موارد النظام. سلسلة حرفية (الحروف الهجائية ، الأرقام ، والرموز الأخرى) تستخدم للتصديق على الهوية أو التحقق من مشروعية تصريح الوصول.	كلمة مرور	Password –

The ability to protect a file using a password access control, protecting the data contents from being viewed with the appropriate viewer unless the proper password is entered.	القدرة على حماية أحد الملفات باستخدام كلمة مرور للتحكم في الوصول إليه . يتم حماية محتوى البيانات من الإطلاع عليها بواسطة برنامج الإطلاع المناسب إلا إذا تم إدخال كلمة المرور الصحيحة.	مُحصَّن بكلمة مرور	Password Protected –
Maintaining an authenticatable record of the prior platforms visited by a mobile software agent, so that a newly visited platform can determine whether to process the agent and what resource constraints to apply.	الاحتفاظ بسجل قابل للتحقق من صحته يضم كل المنصات التي سبق ل برنامج عميل متنقل التعامل معها بحيث يمكن للمنصة الجديدة تحديد إذا كانت هناك حاجة للتعامل مع العميل وما هي القيود المفروضة على الموارد عند التعامل.	البيانات التاريخية لبرنامج عميل متنقل	Path Histories –
A password consisting only of decimal digits. A secret that a claimant memorizes and uses to authenticate his or her identity. PINS are generally only decimal digits. An alphanumeric code or password used to authenticate an identity.	كلمة مرور تتكون فقط من مجموعة أرقام عشرية. سر يحتفظ به مقدم الطلب في ذاكرته ويستخدمه للتصديق على هويته. عادة ما تكون أرقام التعريف الشخصية فقط على شكل أرقام عشرية. شفرة رقمية أو كلمة مرور تُستخدَم في التحقق من الهوية.	رقم التعريف الشخصي	Personal Identification Number (PIN) –
An individual who can act on behalf of an agency to authorize the issuance of a credential to an applicant.	شخص ينوب عن وكالة للتصريح بإصدار عناصر اعتماد المصداقية لأحد المشتركين.	موظف إصدار التصريح بصحة بيانات الهوية الشخصية	Personal Identity Verification Authorizing Official –
Physical artifact (e.g., identity card, “smart” card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation etc.) such that a claimed identity of the cardholder may be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).	بطاقة مصنوعة (مثل بطاقات الهوية والبطاقات الذكية) صادرة لشخص تضم عناصر اعتماد هوية مخزنة (صورة الفوتوغرافية ومفاتيح تشفير وكشف بصمات رقمي) بحيث يمكن التحقق من صحة الهوية التي يدعيها حامل البطاقة بالمقارنة مع عناصر اعتماد المصداقية المخزنة بواسطة شخص أخر (تحقيق هوية يدوي) أو بواسطة إجراء آلي (تحقيق هوية آلي) .	بطاقة التحقق من صحة الهوية الشخصية	Personal Identity Verification Card (PIV Card) –
An authorized identity card creator that procures FIPS approved blank identity cards, initializes them with appropriate software and data elements for the requested identity verification and access control application, personalizes the card with the identity credentials of the authorized subject, and delivers the personalized card to the authorized subject along with appropriate instructions for protection and use.	جهة إصدار بطاقات هوية مُصرَّح بها تقوم بتوريد بطاقات هوية فارغة صادر بشأنها موافقة طبقاً للمعيار الفيدرالي لمعالجة البيانات ثم تشرع في إصدارها مستخدمة برنامج مناسب وعناصر البيانات التي يتطلبها التحقق من الهوية وتطبيق التحكم في الوصول ثم تخصيص البطاقة لشخص معين باستخدام عناصر اعتماد مصداقية الهوية الخاصة به و تُسلَّم البطاقة إليه مع التعليمات المناسبة للحماية والاستخدام.	هيئة إصدار تحقيق الهوية الشخصية	Personal Identity Verification Issuance Authority –
An entity that establishes and vouches for the identity of an applicant to a PIV Issuing Authority. The PIV RA authenticates the applicant’s identity by checking identity source documents and identity proofing and ensures a proper background check has been completed before the credential is issued.	كيان يثبت ويبرهن على شخصية مقدم طلب لهيئة إصدار تحقيق الهوية الشخصية. تقوم هيئة التسجيل بالتحقق من هوية المتقدم بفحص الوثائق الأصلية للهوية وتحقيق الشخصية والتأكد من استكمال خلفيات الموضوع قبل إصدار عناصر اعتماد المصداقية.	هيئة تسجيل تحقيق الهوية الشخصية	Personal Identity Verification Registration Authority –
An individual who can act on behalf of an agency to request a credential for an applicant.	شخص يمكن أن ينوب عن إحدى الوكالات في طلب عناصر اعتماد المصداقية لمقدم طلب	موظف طلب تحقيق الهوية الشخصية	Personal Identity Verification Requesting Official –
Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.	ممارسة الخداع على الأفراد حتى يكشفوا عن معلومات شخصية حساسة من خلال وسائل خداع تعتمد على الحاسوب.	الاصطياد الالكتروني	Phishing –

A network that is not connected to entities or systems outside a physically controlled space.	شبكة لا تتصل بأي كيانات أو أنظمة خارج مساحة السيطرة المادية.	شبكة معزولة مادياً	Physically Isolated Network –
Data input to the Cipher or output from the Inverse Cipher. Intelligible data that has meaning and can be understood without the application of decryption.	مدخلات البيانات إلى عملية الترميز أو مخرجات البيانات من عملية الترميز المعكوس. بيانات واضحة ذات معنى ويمكن فهمها بدون تنفيذ أي فك للتشفير.	نص غير مُشفَّر	Plaintext –
An unencrypted cryptographic key.	مفتاح تشفير غير مُشفَر.	مفتاح غير مُشفَّر	Plaintext Key –
A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.	وثيقة تحدد المهام الواجب إنجازها حيث تبين تفاصيل الموارد المطلوبة لانجاز عناصر الخطة ومراحل استيفاء المهام وتواريخ الانتهاء المجدولة لتلك المراحل.	الخطة التنفيذية والمراحل	Plan of Action and Milestones (POA&M) –
A document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance.	وثيقة تبين هيكلية إدارة الأمن وتحدد بوضوح المسؤوليات الأمنية وتضع الأساس اللازم لقياس الأداء ومدى الالتزام بشكل يُعتمد عليه.	سياسة	Policy –
Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For the FBCA, the PMA is the Federal PKI Policy Authority.	جهاز مُنشأ للإشراف على تكوين وتحديث شهادات السياسات بالإضافة إلى مراجعة بيانات ممارسة التوثيق، ومراجعة نتائج ما تقوم به هيئة التوثيق من تدقيق لمدى الالتزام بالسياسة، وتقييم السياسات التي لا تنتمي للنطاق بغرض ضمها وعموماً فان مهمتها هي مراقبة وإدارة سياسات شهادات البنية التحتية للمفتاح العام. وبالنسبة للهيئة الفيدرالية المشتركة للتوثيق فإن هيئة إدارة السياسات هي الهيئة الفيدرالية لسياسات البنية التحتية للمفاتيح العامة.	هيئة إدارة السياسات	Policy Management Authority (PMA) –
Recognizing that, when a CA in one domain certifies a CA in another domain, a particular certificate policy in the second domain may be considered by the authority of the first domain to be equivalent (but not necessarily identical in all respects) to a particular certificate policy in the first domain.	بملاحظة أنه حينما تقوم هيئة توثيق في أحد النطاقات بمنح الثقة لهيئة توثيق أخرى تنتمي لنطاق مختلف فان هيئة التوثيق في النطاق الأول ربما تعد أحد سياسات التوثيق في النطاق الثاني مشابهة (وليست بالضرورة مماثلة) لأحد سياسات التوثيق الموجودة في النطاق الأول.	تشابه السياسات	Policy Mapping –
A physical entry or exit point of a cryptographic module that provides access to the module for physical signals, represented by logical information flows (physically separated ports do not share the same physical pin or wire).	نقطة دخول أو خروج مادية لوحدة تشفير نمطية توفر للإشارات المادية المتمثلة في التدفق المنطقي للمعلومات إمكانية الوصول لتلك الوحدة النمطية (مع العلم بأن المنافذ المنفصلة مادياً لا تتشارك في نفس موضع التركيب أو السلك) .	منفذ	Port –
Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports).	استخدام برنامج لتحديد المنافذ المفتوحة في أحد الأنظمة عن بعد (مثلاً لمعرفة هل الأنظمة تسمح بإجراء اتصالات من خلال تلك المنافذ) .	فحص المنافذ	Port Scanning –
The loss of confidentiality, integrity, or availability could be expected to have:	فقد السرية أو التكاملية أو استمرارية توفر الخدمة الذي يُتوقَع أن يؤدى إلى:		
1) a limited adverse effect (FIPS 199 low);	1) أثر مضاد محدود (منخفض طبقاً للمعيار الفيدرالي لمعالجة البيانات رقم 199)		
2) a serious adverse effect (FIPS 199 moderate); or	2) أثر مضاد خطير (معتدل طبقاً للمعيار الفيدرالي لمعالجة البيانات رقم 199)		

3) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.	3) أثر مضاد كارثي (مرتفع طبقاً للمعيار الفيدرالي لمعالجة البيانات رقم 199) و ذلك على عمليات المنظمة أو أصولها أو منسوبيها.	التأثير المحتمل	Potential Impact –
A formal statement of the practices followed by an authentication entity (e.g., RA, CSP, or verifier); typically the specific steps taken to register and verify identities, issue credentials and authenticate claimants.	بيان رسمي بالممارسات المتبعة من قِبَل أحد كيانات التصديق (مثل هيئة التسجيل أو موفر خدمة عناصر اعتماد المصداقية أو من يتحقق من صحة البيانات) وبشكل نموذجي هي الخطوات المحددة لتسجيل الهويات والتحقق من صحتها وإصدار عناصر اعتماد المصداقية والتصديق على مقدمي الطلب.	بيان الممارسة	Practice Statement –
A sign that an attacker may be preparing to cause an incident.	علامة ربما يجهزها المهاجم للتسبب في حادثة.	إشارة لبدء الهجوم	Precursor –
An entity whose identity can be authenticated.	كيان يمكن التحقق من صحة هويته.	الكيان الرئيسي	Principal –
The Principal Certification Authority is a CA designated by an Agency to interoperate with the FBCA. An Agency may designate multiple Principal CAs to interoperate with the FBCA.	هي هيئة التوثيق المخصصة من قِبَل إحدى الوكالات للتعامل مع الهيئة الفيدرالية المشتركة للتوثيق. من الممكن أن تخصص الوكالة أكثر من هيئة توثيق رئيسية للتعامل مع الهيئة الفيدرالية المشتركة للتوثيق.	هيئة التوثيق الرئيسية	Principal Certification Authority (CA) –
Restricting access to subscriber or Relying Party information in accordance with Federal law and Agency policy.	تحديد إمكانية الوصول إلى معلومات المشتركين أو الطرف التابع طبقاً للقانونين الحكومية و سياسة الوكالة.	الخصوصية	Privacy –
An analysis of how information is handled:	تحليل لكيفية معالجة المعلومات:		
1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;	1) للتأكد من أن معالجتها تتماشى مع ما يتطلبه قوانين ولوائح وسياسات الخصوصية		
2) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and	2) لتحديد المخاطر والآثار المصاحبة لجمع البيانات والاحتفاظ بها ونشرها بشكل يمكن التعرف عليه في أحد الأنظمة الالكترونية للمعلومات		
3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.	3) لفحص وتقييم وسائل الحماية والعمليات البديلة لمعالجة المعلومات للتخفيف من المخاطر المحتملة التي تهدد الخصوصية.	تقييم تأثير الخصوصية	Privacy Impact Assessment –
The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data. A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public. In an asymmetric (public) cryptosystem, the private key is associated with a public key. Depending on the algorithm, the private key may be used to—	الجزء الخفي لزوج مفتاح غير متناظر يُستخدم بشكل نموذجي في توقيع أو فك تشفير البيانات رقمياً. مفتاح تشفير يستخدم مع خوارزمية تشفير المفتاح العام ويكون مرتبط بشكل فريد غير قابل للتكرار مع أحد الكيانات ولا يعمم استخدامه. في نظام التشفير العام غير المتناظر يعد المفتاح الخاص مرتبطاً بالمفتاح العام. ويمكن استخدام المفتاح الخاص حسب الخوارزمية فيما يلي:		
1) Compute the corresponding public key,	1) حساب المفتاح العام المرتبط به		
2) Compute a digital signature that may be verified by the corresponding public key,	2) حساب التوقيع الالكتروني الذي يمكن التحقق من صحته بالمفتاح العام المرتبط به		
3) Decrypt data that was encrypted by the corresponding public key, or	3) فك تشفير البيانات المُشفرَة بواسطة المفتاح العام المرتبط به		

4) Compute a piece of common shared data, together with other information. A cryptographic key used with a public key cryptographic algorithm, which is uniquely associated with an entity, and not made public; it is used to generate a digital signature; this key is mathematically linked with a corresponding public key. A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public.	4) حساب جزء من البيانات المشتركة إلى جانب معلومات أخرى. مفتاح تشفير يستخدم إلى جانب خوارزمية تشفير المفتاح العام بحيث يتم ربطه مع أحد الكيانات بشكل فريد غير قابل للتكرار ولا يقبل أن يكون عام. يُستخدم في استصدار التوقيع الالكتروني ويكون مرتبط رياضياً بمفتاح تشفير عام. مفتاح تشفير يُستخدم مع خوارزمية تشفير المفتاح العام بحيث يتم ربطه بأحد الكيانات بطريقة فريدة غير قابلة للتكرار ولا يمكن جعله مفتاحاً عاماً.	المفتاح الخاص	Private Key –
Individuals who have access to set “access rights” for users on a given system. Sometimes referred to as system or network administrative accounts.	الإفراد الذين لهم حق الدخول إلى مجموعة من "حقوق الوصول" الخاصة بمستخدمي أحد الأنظمة. في بعض الأحيان يشار لها بالحسابات الإدارية للنظام أو الشبكة.	الحسابات المُمَيَزَة	Privileged Accounts –
Measuring the characteristics of expected activity so that changes to it can be more easily identified.	قياس المواصفات لأحد الأنشطة المتوقعة بحيث يمكن تحديد التغييرات بطريقة أكثر سهولة.	تحديد المواصفات	Profiling –
A protocol where a claimant proves to a verifier that he/she possesses and controls a token (e.g., a key or password).	برتوكول يقوم فيه مقدم الطلب بإثبات ملكيته وتحكمه في إشارة السماح (مفتاح أو كلمة مرور) للمسؤول عن التحقق من الهوية.	برتوكول إثبات الملكية	Proof of Possession Protocol (PoP Protocol) –
Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information.	نظام من خطوط الأسلاك أو الكابلات الضوئية يحتوى على قدر كافي من إجراءات الوقاية و/أو عوامل المقاومة سواء صوتية أو كهربية أو كهرومغناطيسية أو مادية وذلك للسماح باستخدامه في نقل المعلومات غير المشفرة.	نظام التوزيع الوقائي	Protective Distribution System –
A unit of data specified in a protocol and consisting of protocol information and, possibly, user data.	وحدة من البيانات يتم تحديدها في أحد البروتوكولات وتتكون من معلومات عن البروتوكول ومن الممكن بيانات المستخدم.	وحدة بيانات البروتوكول	Protocol Data Unit –
Entity that follows a set of rules and formats (semantic and syntactic) that determines the communication behavior of other entities.	كيان يتبع مجموعة من القواعد والنُسُق (في المعنى و في البنية) التي تحدد طريقة اتصال الكيانات الأخرى.	الكيان المعتمد على بروتوكول	Protocol Entity –
An instance of the exchange of messages between a claimant and a verifier in a defined authentication protocol that results in the authentication (or authentication failure) of the claimant.	حالة لتبادل الرسائل بين مقدم الطلب والمسؤول عن التحقق من الهوية داخل بروتوكول تصديق محدد ينتُج عنه التصديق (أو عدم التصديق) على مقدم الطلب.	تشغيل البروتوكول	Protocol Run –
A proxy is an application that “breaks” the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. This effectively closes the straight path between the internal and external networks. Making it more difficult for an attacker to obtain internal addresses and other details of the organization’s internal network. Proxy servers are available for common Internet services; for example, an Hyper Text Transfer Protocol (HTTP) proxy used for Web access, and an Simple Mail Transfer Protocol (SMTP) proxy used for e-mail.	تطبيق يقوم بفصل قناة الاتصال بين العميل والخادم حيث يقبل الوكيل أنواع معينة من البيانات المتدفقة من وإلى الشبكة ثم يقوم بمعالجتها وتوجيها. يعمل ذلك على غلق الممر المباشر بين الشبكات الداخلية والخارجية بشكل فعَّال مما يزيد الصعوبة التي يواجها المهاجم عند محاولته الحصول على عناوين داخلية أو تفاصيل أخرى عن الشبكة الداخلية للمنظمة. تعد خوادم الوكيل متاحة لخدمات الانترنت الشائعة على سبيل المثال فان وكيل بروتوكول نقل النص المتشعب يُستخدم لتوفير إمكانية الوصول إلى الويب بينما يُستخدم وكيل برتوكول نقل البريد البسيط في البريد الالكتروني.	تطبيق الوكيل (البروكسي)	Proxy –

A proxy agent is a software application running on a firewall or on a dedicated proxy server that is capable of filtering a protocol and routing it to between the interfaces of the device.	تطبيق برمجي يعمل على جدار حماية أو على خادم وكيل مخصص له القدرة على تصفية أحد برتوكولات الاتصال وتوجيهه إلى ما بين وصلات الأجهزة.	عميل الوكيل	Proxy Agent –
A server that sits between a client application, such as a web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.	خادم يقع بين تطبيق العميل مثل متصفح الويب والخادم الحقيقي حيث يعترض كل الطلبات الموجهة إلى الخادم الحقيقي ليرى ما إذا كانت لديه القدرة على الوفاء بتلك الطلبات بنفسه وإلا فانه يقوم بتوجيهها إلى الخادم الحقيقي.	خادم الوكيل	Proxy Server –
An algorithm that produces a sequence of bits that are uniquely determined from an initial value called a seed. The output of the PRNG “appears” to be random, i.e., the output is statistically indistinguishable from random values. A cryptographic PRNG has the additional property that the output is unpredictable, given that the seed is not known.	خوارزمية تقوم بإنتاج سلسة من وحدات البت المحددة بشكل فريد من قيمة مبدئية تسمى "المنشأ". الناتج من مولد الأعداد العشوائية المزيفة "يظهر" كما لو كان عشوائي بمعنى أن الناتج لا يمكن تمييزه إحصائياً عن القيم العشوائية. مولد الأعداد العشوائية المزيفة القادر على التشفير له خاصية إضافية حيث يكون الناتج عنه غير قابل للتوقع بما أن "المنشأ" الخاص به لا يكون معروف.	مولد الأعداد العشوائية المزيفة	Pseudorandom number generator (PRNG) –
A subscriber name that has been chosen by the subscriber that is not verified as meaningful by identity proofing.	اسم المشترك الذي يختاره المشترك ذاته بحيث لا يمكن التحقق من كونه ذو معنى بواسطة إثبات الهوية.	اسم مستعار	Pseudonym –
The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data. A cryptographic key that is used with a public key cryptographic algorithm. The public key is uniquely associated with an entity and may be made public. In an asymmetric (public) cryptosystem, the public key is associated with a private key. The public key may be known by anyone and, depending on the algorithm, may be used to—	الجزء العام من زوج مفتاح غير متناظر يُستخدم في التحقق من صحة التوقيعات أو في تشفير البيانات. مفتاح تشفير يُستخدَم مع خوارزمية تشفير المفتاح العام ويرتبط بشكل فريد غير قابل للتكرار مع أحد الكيانات ويمكن تعميم استخدامه. في نظام التشفير العام غير المتناظر يعد المفتاح العام مرتبطاً بالمفتاح الخاص. ويمكن كشفه لأي فرد واستخدامه طبقاً للخوارزمية فيما يلي:		
1) Verify a digital signature that is signed by the corresponding private key,	1) التحقق من صحة التوقيع الرقمي المستخدم عن طريق المفتاح الخاص المرتبط به		
2) Encrypt data that can be decrypted by the corresponding private key, or	2) تشفير البيانات التي يمكن فك تشفيرها بواسطة المفتاح الخاص المرتبط به		
3) Compute a piece of shared data. A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and which may be made public; it is used to verify a digital signature; this key is mathematically linked with a corresponding private key. A cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public.	3) حساب جزء من البيانات المشتركة. مفتاح تشفير يستخدم مع خوارزمية تشفير المفتاح العام بحيث يتم ربطه مع أحد الكيانات بشكل فريد غير قابل للتكرار ويكون قابل للتعميم. ويُستخدم مفتاح التشفير العام في التحقق من صحة التوقيع الالكتروني ويكون مرتبط رياضياً بأحد مفاتيح التشفير الخاصة. مفتاح تشفير يُستخدم مع خوارزمية تشفير المفتاح العام بحيث يرتبط بأحد الكيانات بطريقة فريدة غير قابلة للتكرار ويمكن تعميمه.	المفتاح العام	Public Key –

A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key. A set of data that unambiguously identifies an entity, contains the entity's public key, and is digitally signed by a trusted third party (certification authority). A set of data that uniquely identifies an entity, contains the entity's public key, and is digitally signed by a trusted party, thereby binding the public key to the entity.	وثيقة رقمية يتم إصدارها وتوقيعها رقمياً بالمفتاح الخاص التابع لهيئة التوثيق التي تربط اسم المشترك مع أحد المفاتيح العامة. الشهادة تشير إلى أن المشترك المذكور فيها له وحده حق التحكم في المفتاح الخاص والوصول إليه. مجموعة من البيانات التي تحدد بوضوح كيان معين حيث تحتوى على المفتاح العام لذلك الكيان وتكون موقعه رقمياً من طرف ثالث موثوق فيه (هيئة التوثيق). مجموعة من البيانات التي تحدد بشكل فريد غير قابل للتكرار كياناً معيناً حيث تحتوى على المفتاح العام لذلك الكيان وتكون موقعه رقمياً من طرف موثوق فيه و بناءاً عليه يُربَط المفتاح العام بذلك الكيان.	شهادة المفتاح العام	Public Key Certificate –
A cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible. Public key cryptography uses “key pairs,” a public key and a mathematically related private key. Given the public key, it is infeasible to find the private key. The private key is kept secret while the public key may be shared with others. A message encrypted with the public key can only be decrypted with the private key. A message can be digitally signed with the private key, and anyone can verify the signature with the public key.	خوارزمية تشفير تستخدم زوج من المفاتيح المترابطة هما المفتاح العام والمفتاح الخاص. يمتلك زوج المفاتيح هذا خاصية أن استنباط المفتاح الخاص من المفتاح العام لا يمكن تحقيقها حاسوبياً. تستخدم طريقة تشفير المفتاح العام "زوج من المفاتيح" هما المفتاح العام الذي يرتبط رياضياً بالمفتاح الخاص. بالحصول على المفتاح العام فإنه من غير الممكن الحصول على المفتاح الخاص ولذلك فان المفتاح الخاص يبقى سراً بينما يمكن مشاركة المفتاح العام مع آخرين. الرسالة المُشفرَة بالمفتاح العام يمكن فك تشفيرها فقط بالمفتاح الخاص. يمكن توقيع أحد الرسائل رقمياً بالمفتاح الخاص كما يمكن لأي شخص التحقق من صحة ذلك التوقيع باستخدام المفتاح العام.	خوارزمية تشفير المفتاح العام (غير المتناظرة)	Public Key (Asymmetric) Cryptographic Algorithm –
A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. An architecture which is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings, and provide other services critical to managing public keys.	مجموعة من السياسات والعمليات ومنصات الخادم والبرمجيات والأجهزة تُستخدم بغرض إدارة الشهادات وأزواج المفتاح العام والخاص بما في ذلك القدرة على إصدار والاحتفاظ وإلغاء شهادات المفتاح العام. هيكلية تُستخدم في ربط المفاتيح العامة بالكيانات وتمكين كيانات أخرى من التحقق من صحة روابط المفتاح العام بالإضافة إلى إمكانية سحب تلك الروابط وتوفير خدمات أخرى ذات أهمية لإدارة المفاتيح العامة.	البنية التحتية للمفتاح العام	Public Key Infrastructure (PKI) –
A starting value for a pseudorandom number generator. The value produced by the random number generator may be made public. The public seed is often called a “salt”.	قيمة مبدئية لمولد الأعداد العشوائية المزيفة. القيمة الصادرة من مولد الأعداد العشوائية الممكن نشرها وجعلها عامة. يعرف المنشأ العام باسم "حد الاطمئنان".	المنشأ العام	Public Seed –
Rendering sanitized data unrecoverable by laboratory attack methods.	جعل البيانات المحذوفة غير قابلة للاسترجاع من خلال أساليب هجوم المعمل.	حذف البيانات نهائياً	Purge –

A process used to generate an unpredictable series of numbers. Each individual value is called random if each of the values in the total population of values has an equal probability of being selected. Random Number Generators (RNGs) used for cryptographic applications typically produce a sequence of zero and one bits that may be combined into sub-sequences or blocks of random numbers. There are two basic classes: deterministic and nondeterministic. A deterministic RNG consists of an algorithm that produces a sequence of bits from an initial value called a seed. A nondeterministic RNG produces output that is dependent on some unpredictable physical source that is outside human control.	عملية تُستخدم في تكوين سلسلة أرقام غير قابلة للتوقع. كل قيمة مفردة في هذه السلسلة تسمى عشوائية إذا كانت القيم في باقي السلسلة لها نفس نسبة الاحتمال في أن يتم اختيارها. يُستخدم مولد الأعداد العشوائي في تطبيقات التشفير لاستصدار سلسلة من وحدات البت صفر وواحد التي يمكن تجميعها في سلسل فرعية أو قوالب من الأعداد العشوائية. يوجد صنفين رئيسين من مولدات الأعداد العشوائية هما: المولد الحتمي والمولد غير الحتمي، فبينما يتكون المولد الحتمي من خوارزمية تنتج سلسلة من وحدات البت اعتمادا على قيمة مبدئية تسمى "المنشأ" فإن المولد غير الحتمي يصدر مخرجات تعتمد على بعض المصادر المادية غير القابلة للتوقع بمعنى أنها خارج السيطرة البشرية.	مولد الأعداد العشوائية	Random Number Generator (RNG) –
The period of time during the cryptoperiod of a symmetric key when protected information is processed. The recipient usage period of the key is usually identical to the cryptoperiod of that key.	هي فترة التشفير التي يستغرقها مفتاح متناظر عند معالجة معلومات محمية. فترة استخدام المُستلِم للمفتاح تكون مماثلة تماماً لفترة التشفير الخاصة بذلك المفتاح.	فترة استخدام المُستلِم	Recipient Usage Period –
The recordings of evidence of activities performed or results achieved (e.g., forms, reports, test results) which serve as the basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).	هي سجلات الأدلة الخاصة بالأنشطة التي تم تنفيذها أو النتائج التي تم تحقيقها مثل النماذج والتقارير ونتائج الاختبارات التي تخدم عملية التحقق من أن المنظمة أو نظام المعلومات يسيران في الاتجاه المرجو. عادة ما تشير السجلات أيضاً إلى وحدات مترابطة من حقول البيانات مثل مجموعات حقول البيانات التي يمكن الوصول إليها ببرنامج يحتوي على مجموعة كاملة من المعلومات عن عناصر معينة.	سجلات	Records –
The security engineering term for IT functionality that—	في هندسة الأمن هو ذلك المصطلح الذي يعبر عن وظيفة تقنية المعلومات التي تتميز بما يلي		
1) controls all access,	1) التحكم في كل عمليات الوصول		
2) cannot be by-passed,	2) استحالة تخطيها		
3) is tamper-resistant, and	3) غير قابلة لإحداث تغييرات غير مصرح بها		
4) provides confidence that the other three items are true.	4) توفر الثقة في أن العناصر الثلاثة سالفة الذكر بالفعل حقيقة.	المراقبة المرجعية	Reference Monitor –
The process through which a party applies to become a subscriber of a Credentials Service Provider (CSP) and a Registration Authority validates the identity of that party on behalf of the CSP.	تلك العملية التي من خلالها يتقدم طرف ليصبح مشترك لدى موفر خدمة عناصر اعتماد التصديق ثم تقوم هيئة التسجيل بالتحقق من صحة الهوية الخاصة بذلك الطرف نيابة عن موفر خدمة عناصر اعتماد التوثيق.	التسجيل	Registration –
A trusted entity that establishes and vouches for the identity of a subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s). Organization responsible for assignment of unique identifiers to registered objects.	كيان يثبت ويبرهن على هوية أحد المشتركين لدى موفر خدمة عناصر اعتماد التصديق. من الممكن أن تكون تلك الهيئة جزء من موفر خدمة عناصر اعتماد التصديق أو تكون مستقلة ولكن على علاقة بموفري خدمة عناصر اعتماد التصديق. منظمة مسؤولة عن منح تعريفات مُميَزة فريدة للعناصر المسجلة.	هيئة التسجيل	Registration Authority (RA) –

To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.	تغيير قيمة مفتاح التشفير المستخدم في تطبيق لأحد أنظمة التشفير وبطبيعة الحال يتطلب ذلك إصدار شهادة جديدة عن المفتاح العام الجديد.	تغيير مفتاح التشفير	Re-key (a certificate) –
An entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to information or a system.	كيان يعتمد على عناصر المصداقية الخاصة بالمشترك لمعالجة أحد التعاملات أو إعطاء حق الوصول إلى معلومات معينة أو نظام معين.	الطرف التابع	Relying Party –
The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, or uninstalling a software application.	تصحيح الثغرات الأمنية وإزالة التهديد. يوجد ثلاثة أنواع محتملة لإصلاح الأخطاء وهي تركيب ملف رقعة أو ضبط إعدادات التهيئة أو إزالة تثبيت البرنامج.	إصلاح الأخطاء	Remediation –
A plan to perform the remediation of one or more threats or vulnerabilities facing an organization's systems. The plan typically includes options to remove threats and vulnerabilities and priorities for performing the remediation.	خطة لتنفيذ إصلاح واحد أو أكثر من التهديدات أو الثغرات الأمنية التي تواجه أنظمة أحد المنظمات حيث تشتمل الخطة عادة خيارات لإزالة التهديدات والثغرات الأمنية بالإضافة إلى ترتيب الأولويات في تنفيذ عملية إصلاح الأخطاء.	خطة إصلاح الأخطاء	Remediation Plan –
Access by users (or information systems) communicating external to an information system security perimeter.	وصول المستخدمين (أو أنظمة معلومات) للاتصال خارجياً بمحيط الأمن الخاص بأحد أنظمة المعلومات.	الوصول عن بعد	Remote Access –
Maintenance activities conducted by individuals communicating external to an information system security perimeter.	أعمال الصيانة التي يجريها أشخاص يتصلون من الخارج بمحيط أمن الخاص أحد أنظمة المعلومات.	الصيانة عن بعد	Remote Maintenance –
The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.	عملية تمديد فترة صلاحية ربط البيانات المدعمة بشهادة مفتاح عام من خلال إصدار شهادة جديدة.	تجديد (شهادة)	Renew (a certificate) –
A database containing information and data relating to certificates as specified in a CP; may also be referred to as a directory.	قاعدة بيانات تحتوى على معلومات وبيانات متعلقة بالشهادات كما حددتها سياسة الشهادة. وقد يُشار إلى مستودع البيانات بكونه أشبه بدليل.	مستودع بيانات	Repository –
The remaining, potential risk after all IT security measures are applied. There is a residual risk associated with each threat.	الجزء المتبقي من المخاطر المحتملة بعد تطبيق كافة مقاييس الأمن. توجد دائماً مخاطر متبقية تتعلق بكل تهديد.	المخاطر المتبقية	Residual Risk –
The entity that responds to the initiator of the authentication exchange.	الكيان الذي يرد على الطرف الذي أنشأ عملية التصديق المتبادل.	جهة الرد	Responder –
A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.	شخص موثوق به يُحدَد من قِبَل إحدى المنظمات المانحة للتصديق على الأفراد المتقدمين للاشتراك طلباً للشهادات بناءاً على تحالفهم مع الجهة المانحة.	شخص مسؤول	Responsible Individual –
To prematurely end the operational period of a certificate effective at a specific date and time.	إلغاء الفترة التشغيلية لشهادة قبل موعد انتهاء صلاحيتها وذلك في تاريخ وزمن محدد.	إلغاء شهادة	Revoke a Certificate –
Cryptographic algorithm specified in the Advanced Encryption Standard (AES).	خوارزمية تشفير مذكورة في المعيار المتقدم للتشفير.	خوارزمية ريجندايل	Rijndael –

The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.	مستوى التأثير الذي تتلقاه عمليات الوكالة (بما في ذلك رسالتها ووظائفها ومصداقيتها وسمعتها) أو أصولها أو منسوبيها نتيجة تشغيل نظام معلومات مع الوضع في الاعتبار التأثير المحتمل لأحد أنواع التهديدات والاحتمالية حدوث ذلك التهديد.	مخاطرة	Risk –
The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.	عملية تشخيص المخاطر التي تهدد أمن النظام وتحديد احتمالية حدوثها والتأثير الناتج عنها وإجراءات الوقاية الإضافية التي تخفف من ذلك التأثير. يعد تحليل المخاطر جزءاً من إدارة المخاطر ومرادفاً لتقييم المخاطر.	تحليل المخاطر	Risk Analysis –
The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.	عملية تشخيص المخاطر التي تهدد عمليات الوكالة (بما في ذلك رسالتها ووظائفها ومصداقيتها وسمعتها) أو أصولها أو منسوبيها من خلال تحديد احتمالية حدوث تلك المخاطر والتأثير الناتج عنها وعناصر التحكم الإضافية التي من شأنها تخفيف ذلك التأثير. يعد تقييم المخاطر جزءاً من إدارة المخاطر ومرادفاً لتحليل المخاطر حيث يعمل على تحليل التهديدات والثغرات الأمنية.	تقييم المخاطر	Risk Assessment –
The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations. The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes:	عملية إدارة المخاطرة التي تهدد أعمال الوكالة (بما في ذلك رسالتها أو وظائفها أو مصداقيتها أو سمعتها) أو أصولها أو منسوبيها نتيجة لتشغيل أحد أنظمة المعلومات. تضم أدارة المخاطر الفروع التالية تقييم المخاطر وتحليل جدوى التكاليف بالإضافة إلى انتقاء وتنفيذ وتقييم عناصر التحكم الأمني والتصريح الرسمي لتشغيل النظام. تضع تلك العملية معايير التأثير والإتقان وكذلك القيود طبقاً للقوانين والتوجيهات والسياسات واللوائح. عملية إدارة المخاطر التي تهدد أعمال المنظمة (بما في ذلك رسالتها أو وظائفها أو مصداقيتها أو سمعتها) وأصولها أو أفرادها نتيجة لتشغيل أحد أنظمة المعلومات. وتضم إدارة المخاطر الفروع التالية:		
1) the conduct of a risk assessment;	1) إجراء تقييم المخاطر		
2) the implementation of a risk mitigation strategy; and	2) تطبيق استراتيجيات التخفيف من المخاطر		
3) employment of techniques and procedures for the continuous monitoring of the security state of the information system. The process of— 1)estimating potential losses due to the use of or dependence upon automated information system technology, 2) analyzing potential threats and system vulnerabilities that contribute to loss estimates, and 3)selecting cost effective safeguards that reduce risk to an acceptable level.	3) استخدام أساليب وإجراءات الرقابة المستمرة للحالة الأمنية لنظام المعلومات . عملية تتضمن ما يلي 1)تقييم الخسائر المحتملة نتيجة استخدام أو الاعتماد على تقنية نظام معلومات آلي 2)تحليل التهديدات المحتملة والثغرات الأمنية في النظام مما يساعد على تقييم الخسائر 3)انتقاء إجراءات الوقاية ذات التكلفة المؤثرة بحيث تقلل من المخاطر إلى مستويات مقبولة.	إدارة المخاطر	Risk Management –

Risk Mitigation –	تخفيف المخاطر	يتضمن تخفيف المخاطر ترتيب الأولويات وتقييم وتطبيق ما هو مناسب من عناصر التحكم في تخفيف المخاطر التي أوصت بها عملية التقييم.	Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process.
Risk Tolerance –	القدرة على احتمال المخاطرة	مستوى المخاطر الذي يتحمله أحد الكيانات بغرض تحقيق أحد النتائج المرجوة المحتملة.	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root Certification Authority –	هيئة التوثيق الأساسية	هي هيئة التوثيق في هيكلية البنية التحتية للمفتاح العام حيث تمتلك المفتاح العام الذي يمثل أكثر البيانات موثوقية (بمعنى أنه بداية طرق منح الثقة) لنطاق الأمن.	In a hierarchical Public Key Infrastructure, the Certification Authority whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Rootkit –	وسائل الوصول الخفي	مجموعة من الأدوات يستخدمها المهاجم بعد تمكنه من الوصول إلى أساس الجهاز المضيف بغرض إخفاء الأنشطة التي يقوم بها مما يسمح للمهاجم الاحتفاظ بقدرته على الوصول إلى أساس الجهاز المضيف بطريق خفية.	A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means.
Round Key –	المفاتيح المتعاقبة	هي قيم مستمدة من مفتاح الترميز باستخدام وظيفة تمديد المفتاح تُطبَق على الترميز والترميز المعكوس.	Round keys are values derived from the Cipher Key using the Key Expansion routine; they are applied to the State in the Cipher and Inverse Cipher.
Rule-Based Security Policy –	سياسة الأمن المعتمدة على القواعد	سياسة أمن تعتمد على القواعد العامة المفروضة على كل الأطراف الفاعلة (المرتبطة بعناصر اعتماد المصداقية). هذه القواعد عادة ما تعتمد على المقارنة بين حساسية العناصر المطلوب الوصول لها وامتلاك الخصائص ذات الصلة من قِبَل الأطراف الفاعلة التي تطلب الوصول.	A security policy based on global rules imposed for all subjects. These rules usually rely on a comparison of the sensitivity of the objects being accessed and the possession of corresponding attributes by the subjects requesting access.
S-box –	صندوق التباديل	جدول تبادل غير خطى يُستخدم في العديد من التحويلات الخاصة بتباديل وحدات البايت ويُستخدم في وظيفة تمديد المفتاح لتنفيذ عملية تبادل أحادية لقيمة من وحدات البايت.	Non-linear substitution table used in several byte substitution transformations and in the Key Expansion routine to perform a one for one substitution of a byte value.
Safeguards –	إجراءات وقائية	قياسات وقائية تُفرَض للوفاء بمتطلبات الأمن (السرية والتكاملية واستمرارية توفر الخدمة) المخصصة الأحد أنظمة المعلومات. من الممكن أن تضم تلك القياسات خصائص أمنية وقيود إدارية وأمن الموظفين وأمن المنشآت المادية والمناطق والأجهزة. لذلك فان عوامل الحماية تعد مرادفاً لعناصر التحكم الأمني وعوامل المقاومة.	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Salt –	حد الملح	قيمة غير سرية تُستخدم فى عملية التشفير عادة بغرض التأكد من أن نتائج الحسابات الخاصة باحد الحالات لن يعاد استخدامها بواسطة احد المهاجمين.	A non-secret value that is used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an attacker.

A method of isolating application modules into distinct fault domains enforced by software. The technique allows untrusted programs written in an unsafe language, such as C, to be executed safely within the single virtual address space of an application. Untrusted machine interpretable code modules are transformed so that all memory accesses are confined to code and data segments within their fault domain. Access to system resources can also be controlled through a unique identifier associated with each domain.	اسلوب لفصل الوحدات النمطية للتطبيق إلى نطاقات أخطاء مُميزة تُفرض بواسطة برنامج. مع البرامج غير الموثوقة والتى تكون مكتوبة بلغات غير مؤمنة مثل لغة سي "C" يسمح هذا الاسلوب بتشغيل آمن لها داخل عنوان افتراضى لأحد التطبيقات. بالنسبة للوحدات النمطية التى يكون لها شفرة آلة قابلة للفهم ولكنها غير موثوقة فانها تخضع للتحويل حتى يتم حصر كل محاولات الدخول للذاكرة داخل نطاقات مخصصة للأخطاء على شكل أجزاء منفصلة من الشفرة والبيانات. يمكن أيضاً السيطرة على الوصول إلى موارد النظام من خلال ربط كل نطاق بأحد عناصر التعريف الفريدة غير القابلة للتكرار.	الصندقة الرملية	Sandboxing –
Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.	عملية لإزالة المعلومات من وسائط التخزين بحيث لا يُمكن استعادتها. يتضمن ذلك نزع كل الملصقات والعلامات وكذلك سجلات النشاط.	حذف البيانات نهائياً	Sanitization –
Sending packets or requests to another system to gain information to be used in a subsequent attack.	إرسال حزم من البيانات أو الطلبات لنظام أخر بغرض الحصول على معلومات لاستخدامها في أحد الهجمات اللاحقة.	فحص الثغرات	Scanning –
Provides organizations with specific technology-related, infrastructure-related, public access-related, scalability-related, common security control-related, and risk-related considerations on the applicability and implementation of individual security controls in the control baseline. Specific factors related to technology, infrastructure, public access, scalability, common security controls, and risk that can be considered by organizations in the applicability and implementation of individual security controls in the security control baseline.	يوفر التوجيه الإرشادي للمنظمات بعض الإرشادات المتعلقة بالتقنية والبنية التحتية والوصول العام والتوسعات المستقبلية وعناصر التحكم الأمني المشترك والمخاطر حول كيفية استخدام وتطبيق عناصر التحكم الأمني الفردية ضمن الحد الأدنى من الرقابة. هو عوامل خاصة تتعلق بالتقنية والبنية التحتية والوصول العام والتوسعات المستقبلية وعناصر التحكم الأمني المشترك والمخاطر التي يمكن للمنظمات وضعها في الاعتبار عند استخدام وتنفيذ عناصر التحكم الأمني الفردية داخل الحد الأدنى من الرقابة الأمنية.	التوجيه الإرشادي	Scoping Guidance –
A cryptographic key that is used with a secret key (symmetric) cryptographic algorithm, that is uniquely associated with one or more entities and is not be made public. The use of the term “secret” in this context does not imply a classification level, but rather implies the need to protect the key from disclosure.	مفتاح تشفير يُستخدم مع خوارزمية تشفير ذات مفتاح سري متناظر بحيث يكون مرتبط بشكل فريد غير قابل للتكرار مع كيان أو أكثر ولا يكمن جعله عام. استخدام مصطلح "سري" في هذا السياق لا يوحي بمستوى من التصنيف ولكن يبين الحاجة لحماية المفتاح من الكشف.	مفتاح سري	Secret Key –
A cryptographic algorithm that uses a single secret key for both encryption and decryption.	خوارزمية تشفير تستخدم مفتاح سرى مفرد للقيام بالتشفير وفك التشفير.	خوارزمية التشفير ذات المفتاح السري المتناظر	Secret Key (symmetric) Cryptographic Algorithm –
A secret value that used to initialize a pseudorandom number generator. The resulting value from the random number generator remains secret or private.	قيمة سرية تُستخدم لإنشاء مولد أعداد عشوائية مزيفة. تبقى القيمة الناتجة من مولد الأعداد العشوائية سرية أو خاصة.	المنشأ السري	Secret Seed –

A set of specifications for securing electronic mail. S/MIME is based upon the widely used MIME standard [MIME] and describes a protocol for adding cryptographic security services through MIME encapsulation of digitally signed and encrypted objects. The basic security services offered by S/MIME are authentication, non-repudiation of origin, message integrity, and message privacy. Optional security services include signed receipts, security labels, secure mailing lists, and an extended method of identifying the signer's certificate(s).	الامتدادات ألآمنة لبريد الانترنت المتعددة الأغراض على معيار امتدادات بريد الانترنت المتعددة الأغراض الشائع الاستخدام وهو يقدم وصفاً لأحد البروتوكولات المستخدمة لإضافة خدمات تشفير أمني إضافية عن طريق تغليف امتدادات بريد الانترنت المتعددة الأغراض للعناصر المشفرة والموقعة رقمياً. الخدمات الأمنية الأساسية التي تقدمها الامتدادات الآمنة لبريد الانترنت المتعددة الأغراض هي خدمات التصديق وعدم إنكار المصدر وتكاملية الرسائل وخصوصية الرسائل كما تضم خدمات اختيارية أخرى هي الإيصالات المُوقعة والملصقات الأمنية وقوائم البريد الآمنة وأسلوب موسع لتحديد من قام بتوقيع الشهادة.	بروتوكول الامتدادات الآمنة لبريد الانترنت متعددة الأغراض	Secure/Multipurpose Internet Mail Extensions (S/MIME) –
A communication protocol that provides the appropriate confidentiality, authentication and content integrity protection	بروتوكول للاتصال يوفر حداً مناسباً من حماية السرية والتصديق وتكاملية المحتوى.	بروتوكول الاتصال الآمن	Secure Communication Protocol –
Secure Sockets Layer is a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. Most web browsers support SSL, and many web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "https:" instead of "http:" TLS is an Internet standard based on SSL version 3.0. There are only very minor differences between SSL and TLS.	سكاب" لنقل الوثائق السرية عبر الانترنت. يعمل ذلك البروتوكول باستخدام مفتاح عمومي لتشفير البيانات المنقولة عبر وصلة طبقة المقابس الآمنة. معظم برامج تصفح الانترنت تدعم استخدام بروتوكول طبقة المقابس الآمنة والكثير من مواقع الويب تستخدمه للحصول على معلومات سرية تخص المستخدم مثل أرقام بطاقات الائتمان. وبطبيعة الحال فان المواقع التي تتطلب قناة اتصال لبروتوكول طبقة المقابس الآمنة تبدأ بـ "https" بدلاً من "http". أما أمن طبقة النقل فانه يمثل معياراً من معايير الانترنت المعتمدة على الإصدار الثالث من بروتوكول طبقة المقابس الآمنة إلا أنه هناك بعض الاختلافات الطفيفة بين بروتوكول طبقة المقابس الآمنة وأمن طبقة النقل.	بروتوكول طبقة المقابس الآمنة وأمن طبقة النقل	Secure Socket Layer and Transport Layer Security (SSL and TSL) –
The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.	قرار الإدارة الرسمية الصادر من أحد الكوادر العليا داخل هيئة ما للتصريح بتشغيل نظام معلومات والقبول علانيةً بتعريض عمليات الهيئة للمخاطرة (بما في ذلك رسالتها ووظائفها ومصداقيتها وسمعتها) وأصولها ومنسوبيها بناءاً على تنفيذ مجموعة من عناصر التحكم الأمني المتفق عليها.	إصدار/اعتماد الموافقة الأمنية	Security Accreditation –
A specification for encoding security assertions in the Extensible Markup Language (XML).	مواصفات لتشفير التأكيدات الأمنية داخل لغة الترميز الممتدة.	لغة ترميز التأكيد الأمني	Security Assertion Markup Language –
A security-related quality of an object. Security attributes may be represented as hierarchical levels, bits in a bit map, or numbers. Compartments, caveats, and release markings are examples of security attributes.	أحد الخواص المتعلقة بأمن أحد العناصر. يمكن تمثيل الخواص الأمنية على شكل مستويات متسلسلة أو وحدات في خريطة لوحدات البت أو أعداد. الأجزاء المستقلة والتوضيحات وعلامات الإصدار تعد من أمثلة الخواص الأمنية .	خاصية أمنية	Security Attribute –

The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.	قرار الإدارة الرسمية الصادر من أحد الكوادر العليا داخل وكالة ما للتصريح بتشغيل نظام معلومات والقبول علانيةً بتعريض عمليات تلك الوكالة للمخاطرة (بما في ذلك رسالتها ووظائفها ومصداقيتها وسمعتها) وأصولها ومنسوبيها بناءاً على تنفيذ مجموعة من عناصر التحكم الأمني المتفق عليها.	التصريح الأمني	Security Authorization –
The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.	وصف للمعلومات أو لأحد أنظمة المعلومات بناءاً على تقييم التأثير المحتمل الذي يحدثه فقد سرية أو تكاملية أو استمرارية توفر المعلومات أو نظام المعلومات على أعمال المنظمة وأصولها ومنسوبيها.	الفئة الأمنية	Security Category –
The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.	أقل مجموعة من عناصر التحكم الأمني المُحددَة لنظام منخفض التأثير أو معتدل التأثير أو مرتفع التأثير.	الحد الأدنى من التحكم الأمني	Security Control Baseline –
Statements of security capability to:	تقارير عن القدرة الأمنية بغرض		
1) build in additional, but related, functionality to a basic control; and/or	1) إنشاء وظائف إضافية (ولكنها مترابطة) للرقابة الأساسية و/أو		Security Control Enhancements –
2) increase the strength of a basic control.	2) زيادة قوة الرقابة الأساسية.	تعزيزات التحكم الأمني	
The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.	عناصر التحكم الإدارية والتشغيلية والتقنية مثل الإجراءات الوقائية وعوامل المقاومة المفروضة على نظام معلومات لحماية سرية وتكاملية واستمرارية توفر النظام وما يحويه من معلومات.	عناصر التحكم الأمني	Security Controls –
A set of subjects, their information objects, and a common security policy. A collection of entities to which applies a single security policy executed by a single authority.	مجموعة من الأطراف الفاعلة وعناصر معلوماتها بالإضافة إلى سياسة أمن مشترك. مجموعة من الكيانات التي تخضع لتطبيق سياسة أمن واحدة تنفذها هيئة واحدة.	النطاق الأمني	Security Domain –
The five security goals are confidentiality, availability, integrity, accountability, and assurance.	الأهداف الخمسة للأمن هي السرية واستمرارية توفر الخدمة والتكاملية والمسؤولية والتأمين.	أهداف الأمن	Security Goals –
The analysis conducted by an agency official, often during the continuous monitoring phase of the security certification and accreditation process, to determine the extent to which changes to the information system have affected the security posture of the system.	هو التحليل الذي يجريه أحد مسؤولي الوكالة ويُنفّذ عادة أثناء مرحلة المراقبة المستمرة لعملية التوثيق الأمني وعملية اعتماد الموافقة بغرض تحديد مدى التأثير الذي أحدثه تغيير بيانات النظام على الوضع الأمني له .	تحليل التأثير الأمني	Security Impact Analysis –
Explicit or implicit marking of a data structure or output media associated with an information system representing the FIPS 199 security category, or distribution limitations or handling caveats of the information contained therein. A marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.	علامة صريحة أو خفية لأحد تركيبات البيانات أو وسائط الإخراج مرتبطة بأحد أنظمة المعلومات لتمثل فئة الأمن من المعيار الفيدرالي لمعالجة البيانات رقم FIPS 199 أو نشر القيود أو التوضيحات حول معالجة محتوى المعلومات. علامة مرتبطة بأحد الموارد (التي من الممكن أن تكون وحدة من البيانات) بحيث تعطي اسماً أو تحدد الخواص الأمنية لذلك المورد.	ملصقات أمنية	Security Label –
A hierarchical indicator of the degree of sensitivity to a certain threat. It implies, according to the security policy being enforced, a specific level of protection.	مؤشر متدرج خاص بدرجات الحساسية تهديد معين. يقوم هذا المؤشر بتوضيح مستوى الحماية طبقاً للسياسة الأمنية المفروضة.	مستوى الأمن	Security Level –

Security Objective –	الغرض الأمني	السرية أو التكاملية أو استمرارية توفر الخدمة.	Confidentiality, integrity, or availability.
Security Policy –	سياسة أمنية	بيان بالحماية المطلوبة لعناصر المعلومات. السياسة الأمنية هي توجيهات الإدارة العليا لإنشاء برنامج أمني قائم على الحاسوب وتحديد أهدافه ومسؤولياته. مجموعة من المعايير الخاصة بشروط الخدمات الأمنية حيث تبين وتحدد الأنشطة الخاصة بمنشأة معالجة بيانات بغرض الحفاظ على حالة من الأمن للأنظمة والبيانات.	The statement of required protection of the information objects. Security Policy is senior management's directives to create a computer security program, establish its goals, and assign responsibilities. A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.
Security Requirements –	متطلبات النظام	المتطلبات المفروضة على أحد أنظمة المعلومات و المستمدة من القوانين أو الأوامر التنفيذية أو التوجيهات أو السياسات أو التعليمات أو الاحتياجات (التشغيلية) للمنظمة بغرض التأكد من سرية وتكاملية واستمرارية توفر المعلومات التي يتم معالجتها وتخزينها ونقلها.	Requirements levied on an information system that are derived from laws, executive orders, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Security Service –	خدمة أمنية	أحد الإمكانيات التي تدعم واحد أو أكثر من الأهداف الأمنية. من أمثلة الخدمات الأمنية مفاتيح الإدارة والتحكم في الوصول والتصديق.	A capability that supports one, or many, of the security goals. Examples of security services are key management, access control, and authentication.
Security Tag –	البطاقات الأمنية	أحد وحدات المعلومات التي تحوي عرضاً لبيانات محددة تتعلق بالأمن مثل خريطة الخصائص الحصرية لوحدات البت.	Information unit containing a representation of certain security-related information (e.g., a restrictive attribute bit map).
Senior Agency Information Security Officer –	الموظف المسؤول عن أمن المعلومات داخل الوكالة	موظف مسؤول تنفيذ مسؤوليات رئيس قطاع المعلومات التي حددها القانون الفيدرالي لإدارة أمن المعلومات ويكون همزة الوصل الرئيسية بين رئيس قطاع المعلومات وموظفي التصريحات داخل الوكالة ومالكي نظام المعلومات وموظفي بيانات أمن نظام المعلومات.	Official responsible for carrying out the Chief Information Officer responsibilities under the Federal Information Security Management Act (FISMA) and serving as the Chief Information Officer’s primary liaison to the agency’s authorizing officials, information system owners, and information system security officers.
Sensitivity –	حساسية البيانات	تستخدم في هذا الدليل الإرشادي لتعني مقياس للأهمية المُعطَاة للمعلومات من قِبَل مالكها بغرض إظهار مدى احتياجها للحماية.	Used in this guideline to mean a measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.
Sensitivity Levels –	مستويات الحساسية	نظام تدريجي يمنح علامات (منخفض ، معتدل ، مرتفع) للمعلومات أو أنظمة معالجة المعلومات بناءاً على التهديدات والمخاطر الناتجة في حالة تنفيذ أحد التهديدات بنجاح.	A graduated system of marking (e.g., low, moderate, high) information and information processing systems based on threats and risks that result if a threat is successfully conducted.
Shared Secret –	سر مشترك	سر يُستخدَم في عملية التصديق بحيث يكون معروف لمقدم الطلب والمسؤول عن التحقق من صحة الهوية.	A secret used in authentication that is known to the claimant and the verifier.
Signature –	توقيع	نموذج معروف ومُميَّز مرتبط بأحد الهجمات مثل السلسلة الثائية في أحد الفيروسات أو مجموعة معينة من ضربات لوحة المفاتيح التي تُستخدم للحصول على وصول غير مصرح به إلى النظام.	A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.
Signature Certificate –	شهادة توقيع	شهادة مفتاح عام تحتوى على مفتاح عام مخصص للتحقق من التوقيعات الرقمية بدلاً من تشفير البيانات أو تنفيذ أي وظائف تشفير أخرى.	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

Signature Generation –	استصدار التوقيع	استخدام خوارزمية توقيع رقمي ومفتاح خاص لاستصدار توقيع رقمي على البيانات.	Uses a digital signature algorithm and a private key to generate a digital signature on data.
Signature Verification –	التحقق من صحة التوقيع	استخدام خوارزمية توقيع رقمي ومفتاح عام للتحقق من صحة أحد التوقيعات الرقمية.	Uses a digital signature algorithm and a public key to verify a digital signature.
Signed Data –	بيانات موقّعة	بيانات تم استصدار توقيع رقمي عليها.	Data on which a digital signature is generated.
Single-Hop Problem –	مشكلة متنقلة	المخاطر الأمنية الناتجة من أحد عملاء البرامج المتنقلة الذي يتحرك من منصته الابتدائية إلى منصة أخرى.	The security risks resulting from an mobile software agent moving from its home platform to another platform.
Smart Card –	بطاقة ذكية	بطاقة ائتمان مزودة بمعالج دقيق وشريحة ذاكرة تُستخدَم في التحقق من الهوية والتعاملات المالية. عند إدخالها لجهاز قارئ البطاقات الذكية تقوم البطاقة بنقل البيانات من وإلى أحد أجهزة الحاسوب المركزية. البطاقة الذكية أكثر أمناً من بطاقة الشريط الممغنط ويمكن برمجتها لتدمر نفسها ذاتياً في حال تعددت مرات إدخال كلمة المرور بطريقة خاطئة.	A credit card with a built-in microprocessor and memory that is used for identification or financial transactions. When inserted into a reader, the card transfers data to and from a central computer. A smart card is more secure than a magnetic stripe card and can be programmed to self-destruct if the wrong password is entered too many times.
Sniffer –	ملتقط حزم البيانات	برنامج يقوم بملاحظة وتسجيل حركة التدفق عبر الشبكة.	Software that observes and records network traffic.
Social Engineering –	الهندسة الاجتماعية	محاولة لخداع شخص لكي يكشف عن معلومات (كلمة مرور مثلاً) بغرض استخدامها في الهجوم على الأنظمة أو الشبكات.	An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.
Software-Based Fault Isolation –	فصل الأخطاء غير الآمنة	أسلوب لفصل الوحدات النمطية للتطبيق إلى نطاقات خطأ مُميزَة تم فرضها بواسطة برنامج. مع البرامج غير الموثوقة والتي تكون مكتوبة بلغات غير مؤمنة مثل لغة سي "C" يسمح هذا الأسلوب بتشغيل آمن لها داخل عنوان افتراضي لأحد التطبيقات. بالنسبة للوحدات النمطية التي يكون لها شفرة آلة قابلة للفهم ولكنها غير موثوقة فإنها تخضع للتحويل حتى يتم حصر كل محاولات الدخول للذاكرة داخل نطاقات مخصصة للأخطاء على شكل أجزاء منفصلة من الشفرة والبيانات. يمكن أيضاً السيطرة على الوصول إلى موارد النظام من خلال ربط كل نطاق بأحد عناصر التعريف الفريدة غير القابلة للتكرار.	A method of isolating application modules into distinct fault domains enforced by software. The technique allows untrusted programs written in an unsafe language, such as C, to be executed safely within the single virtual address space of an application. Untrusted machine interpretable code modules are transformed so that all memory accesses are confined to code and data segments within their fault domain. Access to system resources can also be controlled through a unique identifier associated with each domain.

A procedure whereby a cryptographic key is handled as multiple key components from the time that the key or the separate key components are generated until the key components are combined for use. Each key component provides no knowledge of the ultimate key. The key may be created and then split into the key components, or may be created as separate key components. The key components are output from the generating cryptographic module(s) to separate entities for individual handling, and subsequently input separately into the intended cryptographic module and combined to form the ultimate key. Note: A suitable combination function is not provided by simple concatenation; e.g., it is not acceptable to form an 80-bit key by concatenating two 40-bit key components. A process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, that can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key.	إجراء بموجبه يتم التعامل مع أحد مفاتيح التشفير على أنه مكونات مفتاح متعددة من وقت استصدار المفتاح أو مكونات المفتاح المنفصلة حتى يتم تجميع مكونات المفتاح بغرض الاستخدام. كل مكون من مكونات المفتاح لا يعطي أية بيانات عن المفتاح الكامل. يمكن إنشاء المفتاح ثم تفكيكه إلى مكونات أو يمكن إنشاءه من البداية على شكل مكونات مفتاح منفصلة. مكونات المفتاح هي ناتج من وحدات التشفير النمطية بغرض فصل الكيانات لمعالجتها على إنفراد ثم إدخالها منفصلة إلى الوحدة النمطية المقصودة وجمعها لتكون المفتاح الكامل. ملحوظة: دالة التجميع المناسبة ليست مجرد ربط تسلسلي بسيط إذ أنه من غير المقبول تكوين مفتاح طوله 80 من وحدات البت بمجرد تكوين سلسلة تضم اثنين من مكونات المفتاح ذوى 40 من وحدات البت. عملية يتم فيها تفتيت أحد مفاتيح التشفير إلى مكونات مفتاح متعددة لا تتشارك فيما بينها في أية معرفة بالمفتاح الأصلي بحيث يمكن لاحقاً إدخالها إلى أو إخراجها من أحد وحدات التشفير النمطية من خلال كيانات منفصلة وتجميعها لإعادة إنشاء مفتاح التشفير الأصلي.	تجزئة مفتاح التشفير	Split Knowledge –
“IP spoofing” refers to sending a network packet that appears to come from a source other than its actual source. Involves—	يشير "خداع بروتوكول الانترنت" إلى إرسال حزمة بيانات عبر شبكة بحيث تبدو إنها تأتى من مصدر غير مصدرها الفعلي ويتضمن ذلك		
1) the ability to receive a message by masquerading as the legitimate receiving destination, or	1) القدرة على استقبال رسالة من خلال التنكر كما لو كان هو مقر الوصول الشرعي للتسليم أو		
2) masquerading as the sending machine and sending a message to a destination.	2) التنكر كما لو كان الجهاز المرسل ثم يرسل رسالة إلى أحد جهة الاستلام.	خداع بروتوكول الانترنت	Spoofing –
Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.	برامج مثبتة في أحد أنظمة المعلومات سراً أو خلسة لجمع المعلومات عن الأفراد أو المنظمات دون علمهم أي انه أحد أنواع الشفرة الخبيثة.	برامج تجسس	Spyware –
A published statement on a topic specifying characteristics, usually measurable, that must be satisfied or achieved in order to comply with the standard.	بيان منشور حول موضوع يحدد تلك المواصفات - التي عادة تكون قابلة للقياس - الواجب استيفاءها أو تحقيقها للتماشي مع ذلك المعيار.	معيار / مقياس	Standard –
The format and information required to be displayed on a PIV card. Also known as the Mandatory Topography.	النسق والمعلومات المطلوب عرضها على بطاقة التعريف الشخصي. ويطلق عليها أيضاً بيانات التعريف الإجبارية.	بيانات التعريف الأساسية	Standard Topography –
Intermediate Cipher result that can be pictured as a rectangular array of bytes.	نتيجة ترميز وسيطة يمكن تصويرها على شكل مصفوفة مستطيلة من وحدات البايت.	الحالة الوسيطة للترميز	State –
Static keys are relatively long-lived and are common to a number of executions of a given algorithm.	مفاتيح تكون طويلة الأمد نسبياً وتتميز بشيوعها بين عدد من عمليات تنفيذ أحد الخوارزمية.	مفاتيح ثابتة	Static Keys –

The art and science of communicating in a way that hides the existence of the communication. For example, a child pornography image can be hidden inside another graphic image file, audio file, or other file format.	هو علم الاتصال بطريقة تُخفي وجود ذلك الاتصال على سبيل المثال يمكن إخفاء أحد الصور الإباحية داخل ملف صورة أو ملف صوتي أو أي نسق من أنواع الملفات الأخرى.	علم إخفاء الاتصال (ستيجانوجرافي)	Steganography –
The person whose identity is bound to a particular credential.	هو الشخص الذي ترتبط هويته بعناصر اعتماد مصداقية معينة.	الطرف الفاعل	Subject –
In a hierarchical PKI, a Certification Authority whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA.	هي هيئة توثيق - ضمن هيكلية البنية التحتية للمفتاح العام - يكون مفتاح توقيع الشهادة الخاص بها موثقاً من قبل هيئة توثيق أخرى كما تكون أنشطتها مقيدة بتلك الهيئة.	هيئة التوثيق الفرعية	Subordinate Certification Authority (CA) –
A party who receives a credential or token from a CSP and becomes a claimant in an authentication protocol.	الطرف الذي يستلم عناصر اعتماد المصداقية أو إشارة السماح من موفر خدمة عناصر اعتماد المصداقية وبذلك يصبح مقدم الطلب بالنسبة لأحد بروتوكولات التصديق.	مشترك	Subscriber –
A major subdivision or component of an information system consisting of information, information technology, and personnel that perform one or more specific functions.	أحد الأقسام الفرعية أو المكونات الكبيرة لنظام معلومات يضم معلومات وتقنية معلومات وموظفين تقوم بتنفيذ مهمة محددة أو أكثر.	نظام فرعي	Subsystem –
In a hierarchical PKI, a Certification Authority who has certified the certificate signature key of another CA, and who constrains the activities of that CA.	هي هيئة توثيق - ضمن هيكلية البنية التحتية للمفتاح العام - والتي تقوم بتوثيق مفتاح توقيع الشهادة لهيئة توثيق أخرى كما تكون هي المقيِّدّة لأنشطة تلك الهيئة.	هيئة التوثيق العليا	Superior Certification Authority
Encryption algorithms using the same secret key for encryption and decryption.	خوارزميات تشفير تستخدم نفس المفتاح السري للقيام بعمليتي التشفير وفك التشفير.	خوارزمية التشفير المتناظرة	Symmetric Encryption Algorithm –
A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code. A single cryptographic key that is used with a secret (symmetric) key algorithm.	مفتاح تشفير يُستخدم لتنفيذ عملية تشفير ومعكوسها على سبيل المثال القيام بالتشفير وفك التشفير أو إنشاء شفرة رسالة تصديق والتحقق من صحتها. مفتاح تشفير مفرد يُستخدَم مع أحدى خوارزمية مفتاح سري متناظر.	مفتاح متناظر	Symmetric Key –
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.	مجموعة من موارد المعلومات المنفصلة مُرتبة بغرض تجميع أو معالجة أو صيانة أو استخدام أو مشاركة أو توزيع أو التخلص من المعلومات.	نظام	System –
A person who manages the technical aspects of a system.	هو الشخص الذي يدير النواحي التقنية لأحد الأنظمة.	مدير النظام	System Administrator –
The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.	مدى الأنشطة المرتبطة بالنظام والتي تضم إنشاء النظام وتطويره وامتلاكه وتنفيذه وتشغيله وصيانته والتخلص منه بالكامل بحيث يدفع إلى البدء في إنشاء نظام أخر.	دورة حياة النظام	System Development Life Cycle (SDLC) –
The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.	هي تلك الميزة التي يمتلكها النظام عند تنفيذه للوظيفة المقصودة منه بطريقة لا يشوبها أي تقصير، بطريقة خالية من أي تلاعب غير مصرح به سواء كان تلاعب مقصود أو غير مقصود.	تكاملية/سلامة/وحدة النظام	System Integrity –
The direct connection of two or more IT systems for the purpose of sharing data and other information resources.	الاتصال المباشر بين اثنين أو أكثر من أنظمة المعلومات بغرض مشاركة البيانات وموارد المعلومات الأخرى.	ترابط النظام	System Interconnection –
A security control for an information system that has not been designated as a common security control.	عنصر تحكم أمني مخصص لأحد أنظمة المعلومات حيث لم يُصنف على أساس كونه عنصر تحكم أمني مشترك.	عنصر التحكم الأمني المخصص لنظام معين	System-specific Security Control –

Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.	وثيقة رسمية تعطي نظرة شاملة لمتطلبات أمن نظام معلومات وتقدم توصيف لعناصر التحكم الأمني الموجودة بالفعل أو المخطط توفيرها حتى يتم الوفاء بتلك المتطلبات.	خطة أمن النظام	System Security Plan –
The special software within the cryptographic boundary (e.g., operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, and associated programs, and data.	تلك البرامج الخاصة الموجودة داخل حدود التشفير (مثلاً أنظمة التشغيل أو برامج المترجم أو برامج الأدوات) المُصممة لنظام حاسوبي معين أو مجموعة من أنظمة الحاسوب بغرض تيسير تشغيل وصيانة نظام الحاسوب والبرامج المرافقة له وكذلك البيانات الموجودة عليه.	برامج النظام	System Software –
The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.	عناصر التحكم الأمنية مثل إجراءات الوقاية وعوامل المقاومة الخاصة بأحد أنظمة المعلومات والتي يُطبقها ويُنفذها نظام المعلومات عن طريق آليات موجودة في مكونات النظام من أجهزة وبرمجيات وبرامج تشغيل مثبتة في ذاكرة القراءة.	عناصر الرقابة التقنية	Technical Controls –
The contribution of public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.	المساعدة التي تقدمها آليات المفتاح العام لتوفير الدليل التقني الذي يدعم الخدمة الأمنية لعدم الإنكار.	عدم الإنكار التقني	Technical non-repudiation –
A name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment.	مصطلح يشير إلى البحث والدراسة والرقابة لظواهر الانتهاكات الأمنية غير المقصودة من أجهزة الاتصالات وأنظمة المعلومات الآلية.	العاصفة	Tempest –
A biometric image data record.	سجل بيانات لصورة قياس حيوي.	نموذج /قالب جاهز	Biometric Template –
Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	أي ظرف أو حدث من المحتمل أن يؤثر تأثيراً معادياً على أعمال الوكالة (بما في ذلك مهمتها أو وظائفها أو مصداقيتها أو سمعتها) أو أصولها أو منسوبيها مستغلاً أحد أنظمة المعلومات عن طريق الوصول غير المصرح به إلى المعلومات أو تدميرها أو كشفها أو تغييرها و/أو حجب الخدمة . وأيضاً قدرة مصدر التهديد على النجاح في استغلال أحد نقاط الضعف الخاصة بنظام معلومات معين.	تهديد	Threat –
Either:	هو إما		
1) intent and method targeted at the intentional exploitation of a vulnerability; or	1) نية وأسلوب يهدف لاستغلال المقصود أحد الثغرات الأمنية عن قصد أو		
2) a situation and method that may accidentally trigger a vulnerability.	2) موقف وأسلوب يُحدث ثغرة أمنية دون قصد.	مصدر التهديد	Threat Agent/Source –
The examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.	فحص مصادر التهديد الموجَّهة للثغرات الأمنية في النظام لتحديد التهديدات التي تحيط بنظام معين داخل بيئة تشغيل معينة.	تحليل التهديد	Threat Analysis –
Formal description and evaluation of threat to an information system.	وصف وتقييم منهجي للتهديد الموجه ضد أحد أنظمة المعلومات.	تقييم التهديد	Threat Assessment –

Something that the claimant possesses and controls (typically a key or password) used to authenticate the claimant's identity.	شئ (عادة ما يكون مفتاح أو كلمة مرور) يمتلكه مقدم الطلب ويتحكم فيه بحيث يستخدم فى التصديق على هوية مقدم الطلب.	اشارة السماح / رمز مُميِّز	Token –
The physical, non-logical features of a card. A card may have either standard or enhanced topography.	الخصائص المادية غير المنطقية لبطاقة. يمكن أن يكون للبطاقة طوبولوجيا عادية أو أخرى متقدمة.	طوبولوجيا خصائص البطاقة	Topology –
The potential for the occurrence of an adverse event if no mitigating action is taken (i.e., the potential for any applicable threat to exploit a system vulnerability).	احتمال وقوع حدث مُعادي إذا لم تُتَخَذ أية إجراءات للتخفيف بمعنى احتمال قيام أي تهديد باستغلال أحد الثغرات الأمنية بالنظام.	مجموع المخاطر	Total Risk –
A cookie placed on a user's computer to track the user's activity on different Web sites, creating a detailed profile of the user's behavior.	ملف لجمع البيانات يوضع على حاسوب المُستخدم لتتبع نشاطه عبر مواقع الويب المختلفة لإنشاء ملف مفصل بخصائص تصرف هذا المُستخدِم .	تتبع ملفات (كعكة) جمع البيانات	Tracking Cookie –
A form of passive attack in which an intruder observes information about calls (although not necessarily the contents of the messages) and makes inferences, e.g. from the source and destination numbers, or frequency and length of the messages.	شكل من أشكال الهجوم السلبي حيث يقوم فيه المتسلل بمراقبة معلومات طلب الاتصال (بالرغم من أنها ليست بالضرورة محتويات الرسائل) ثم يقوم بعمل استنتاجات على سبيل المثال من الأرقام الخاصة بمصدر الرسائل ومكان وصولها أو ترددها وطولها.	تحليل تدفق البيانات	Traffic Analysis –
Training strives to produce relevant and needed (information) security skills and competencies.	يسعى التدريب إلى إخراج المهارات والكفاءات ذات الصلة التي يتطلبها أمن المعلومات.	التدريب على أمن المعلومات	Training (Information Security) –
An evaluation of the training efforts.	تقييم للجهود المبذولة في التدريب.	تقييم التدريب	Training Assessment –
A measurement of what a given student has learned from a specific course or training event.	قياس لما تعلمه أحد الطلبة من أحد المقررات التعليمية أو أحد دورات التدريب.	فعالية التدريب	Training Effectiveness –
Information collected to assist employees and their supervisors in assessing individual students' subsequent on-the-job performance, to provide trend data to assist trainers in improving both learning and teaching, and to be used in return-on-investment statistics to enable responsible officials to allocate limited resources in a thoughtful, strategic manner among the spectrum of IT security awareness, security literacy, training, and education options for optimal results among the workforce as a whole.	معلومات مجمَّعة لتساعد الموظفين ومديريهم في تقييم أداء الطلبة أثناء العمل كلٍ على حدا بغرض توفير بيانات تساعد المدربين في تحسين طرق التعليم والتدريس لاستخدامها في إحصائيات تمكن المسؤولين من توزيع الموارد المحدودة بطريقة ذكية وإستراتيجية بين مجالات الوعي بأمن تقنية المعلومات ومحو أمية الأمن والتدريب وخيارات التعليم للوصول بقوة العمل كلها إلى أفضل النتائج.	تقييم فعالية التدريب	Training Effectiveness Evaluation –
An authentication and security protocol widely implemented in browsers and web servers.	بروتوكول للتصديق والأمن يشيع استخدامه في متصفحات وخوادم الويب.	بروتوكول طبقة النقل	Transport Layer Security (TLS) –
An implementation of the Data Encryption Standard (DES) algorithm that uses three passes of the DES algorithm instead of one as used in ordinary DES applications. Triple DES provides much stronger encryption than ordinary DES but it is less secure than AES.	تطبيق لخوارزمية معيار تشفير البيانات باستخدام ثلاث مسارات لخوارزمية معيار تشفير البيانات بدلاً من استخدام واحدة فقط كما في التطبيقات العادية لمعيار تشفير البيانات. يوفر معيار التشفير الثلاثي للبيانات تشفيراً أكثر قوة من المعيار العادي ولكنه أقل أمناً من المعيار المتقدم للتشفير.	معيار التشفير الثلاثي للبيانات	Triple DES –
A non-self-replicating program that seems to have a useful purpose, but in reality has a different, malicious purpose.	برنامج لا يقوم بنسخ نفسه حيث يتظاهر بكونه ذو أغراض مفيدة ولكنه في الحقيقة يخفى غرض خبيث.	حصان طروادة	Trojan Horse –

A public key and the name of a certification authority that is used to validate the first certificate in a sequence of certificates. The trust anchor public key is used to verify the signature on a certificate issued by a trust anchor certification authority. The security of the validation process depends upon the authenticity and integrity of the trust anchor. Trust anchors are often distributed as self-signed certificates.	مفتاح عام واسم هيئة توثيق يُستخدمان في التحقق من صلاحية الشهادة الأولى في سلسلة من الشهادات. يُستخدَم إثبات الثقة في التحقق من صحة التوقيع الموجود على الشهادة الصادرة من إحدى هيئات توثيق إثبات الثقة. يعتمد أمن عملية التحقق من صلاحية على المصداقية والتكاملية الخاصة بإثبات الثقة. إثباتات الثقة عادة ما تكون موزعة على شكل شهادات موقعة ذاتياً.	إثبات الثقة	Trust Anchor –
The collection of trusted certificates used by Relying Parties to authenticate other certificates.	مجموعة من شهادات موثوقة تستخدمها الأطراف التابعة للتصديق على شهادات أخرى.	قائمة الثقة	Trust List –
Entity authorized to act as a representative of an Agency in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.	كيان مصرَّح به ينوب عن وكالة في تأكيد هوية مشترك أثناء عملية التسجيل. الوكيل المعتمد ليس لديه قنوات اتصال آلية مع هيئات التوثيق.	الوكيل المعتمد	Trusted Agent –
A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".	شهادة موثوق بها من طرف تابع بناءاً على التسليم الآمن والمصدق عليه. المفاتيح العامة الموجودة في الشهادات المُعتمدَة تُستخدَم لبدء مسارات التوثيق. وتعرف تلك الشهادات أيضا بـ "إثبات الثقة".	شهادة مُعتمدَة	Trusted Certificate –
A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software. A means by which an operator and a target of evaluation security function can communicate with the necessary confidence to support the target of evaluation security policy.	آلية تتيح للمستخدم (من خلال أداة إدخال) أن يتصل مباشرة مع الوظائف الأمنية لنظام معلومات في إطار من الثقة الضرورية لدعم سياسة أمن النظام. هذه الآلية يمكن فقط تنشيطها بواسطة المستخدِم أو وظائف الأمنية لنظام المعلومات ولا يمكن تقليدها باستخدام برمجيات غير موثوقة. وسيلة يمكن بها إقامة اتصال بين أحد المشغلين وهدف لوظيفة تقييم أمنية في إطار من الثقة المطلوبة لدعم الغرض من سياسة التقييم الأمنية.	مسار موثوق	Trusted Path –
A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.	تأكيد مُوقَّع رقمياً من قِبَل هيئة معتمدة بأن عنصر رقمي معين كان موجود في وقت معين.	ختم الوقت المعتمد	Trusted Timestamp –
The attribute of a person or organization that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.	خاصية لأحد الأشخاص أو المنظمات تمنح الثقة للآخرين حول المؤهلات والقدرات والاعتمادية التي يتمتع بها كيان لتنفيذ مهام معينة وللوفاء بمسؤوليات محددة.	الثقة	Trustworthiness –
Computer hardware, software and procedures that—	معدات حاسوب و برمجيات و إجراءات تتمتع بما يلي		
1) are reasonably secure from intrusion and misuse;	1) مستوى معقول من الأمن ضد الاختراق أو إساءة الاستخدام		
2) provide a reasonable level of availability, reliability, and correct operation;	2) مستوى معقول من استمرارية توفر الخدمة والاعتمادية والتشغيل السليم		
3) are reasonably suited to performing their intended functions; and	3) مُهيأة بدرجة معقولة لأداء وظائفها		
4) adhere to generally accepted security procedures.	4) بكونها مُلتزمة بالإجراءات الأمنية المقبولة بشكل عام.	نظام موثوق	Trustworthy System –

A protocol where a password is sent through a protected channel. For example, the TLS protocol is often used with a verifier's public key certificate to	بروتوكول تُرسل فيه كلمة المرور من خلال قناة اتصال محمية. على سبيل المثال فان بروتوكول طبقة النقل عادة ما يُستخدم مع شهادة مفتاح عام تخص المسؤول عن التحقق من الهوية لعمل الأتي		
(1) authenticate the verifier to the claimant,	1) تصديق المسؤول عن التحقق من هوية مقدم الطلب		
(2) establish an encrypted session between the verifier and claimant, and	2) إنشاء فترة تعامل مُشفرَة مع النظام بين المسؤول عن التحقق من الهوية ومقدم الطلب		
(3) transmit the claimant's password to the verifier. The encrypted TLS session protects the claimant's password from eavesdroppers.	3) نقل كلمة المرور الخاصة بمقدم الطلب إلى المسؤول عن التحقق من الهوية. تعمل فترة التعامل مع النظام المشفرة باستخدام بروتوكول طبقة النقل على حماية كلمة المرور الخاصة بمقدم الطلب من المتصنتين على الأنظمة .	بروتوكول كلمة المرور المحمية	Tunneled Password Protocol –
A person gains logical or physical access without permission to a network, system, application, data, or other resource. It occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use.	أحد الأشخاص يحصل على وصول منطقي أو مادي إلى شبكة أو نظام أو تطبيق أو بيانات أو موارد أخرى دون إذن بذلك. يحدث ذلك عندما يقوم أحد المستخدمين سواء كان مستخدم شرعي أو غير مصرح له بالوصول إلى أحد الموارد التي ليس له الحق في استخدامها .	الوصول غير المصرح به	Unauthorized Access –
An event involving the exposure of information to entities not authorized access to the information.	حدث يتضمن كشف المعلومات لجهات غير مصرح لها الوصول إليها.	كشف غير مصرح به للبيانات	Unauthorized Disclosure –
Data included in an authentication token, in addition to a digital signature.	بيانات موجودة في إشارة سماح للتصديق بالإضافة إلى التوقيع الالكتروني.	بيانات غير مُوقعَة	Unsigned data –
The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.	عملية تخضع فيها عناصر البيانات الموجودة في شهادة مفتاح عام (خاصة بيانات التصريحات الممنوحة لأحد الأطراف الفاعلة) إلى التغيير عن طريق إصدار شهادة جديدة.	تحديث (شهادة رقمية)	Update (a Certificate) –
Individual or (system) process authorized to access an information system. An individual or a process (subject) acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services.	أحد الأفراد أو عمليات (النظام) مصرح له الوصول إلى أحد أنظمة المعلومات. أحد الأفراد أو العمليات (طرف فاعل) ينوب عن الشخص الذي له حق الوصول إلى أحد وحدات التشفير النمطية بغرض الحصول على خدمات مُشفرَة.	مُستخدَم	User –
A stage in the lifecycle of keying material; the process whereby a user initializes its cryptographic application (e.g., installing and initializing software and hardware).	مرحلة في دورة تكوين مفتاح التشفير بموجبها يقوم المستخدم بإنشاء تطبيقه المُشفَّر (مثلاً تثبيت وإعداد برنامج أو أحد الأجهزة) .	إنشاء مُستخدِم	User Initialization –
A stage in the lifecycle of keying material; a process whereby an entity becomes a member of a security domain.	مرحلة في دورة تكوين مفتاح التشفير بموجبها يصبح أحد الكيانات عضواً في أحد النطاقات الأمنية.	تسجيل مستخدم	User Registration –
A payload, an associated data string, or a nonce that satisfies the restrictions of the formatting function.	البيانات المرسلة عبر الشبكة أو سلسلة البيانات المرفقة أو القيم المؤقتة التي تفي بالقيود الخاصة بوظيفة التنسيق.	عنصر بيانات صحيح	Valid Data Element –
The process of demonstrating that the system under consideration meets in all respects the specification of that system.	عملية تبين أن النظام موضع الاهتمام يلبى كافة المواصفات المطلوبة في جميع الجوانب.	التحقق من الصلاحية	Validation –
The process of affirming that a claimed identity is correct by comparing the offered claims of identity with previously proven information stored in the identity card or PIV system.	التأكد من صحة الهوية التي تم إدعاءها عن طريق المقارنة بين إدعاءات الهوية المقدمة والمعلومات الصحيحة المخزنة سلفاً في بطاقة الهوية أو نظام التحقق من صحة الهوية الشخصية .	التحقق من الهوية	Verification –
A subscriber name that has been verified by identity proofing.	اسم مشترك جرى التحقق من هويته باستخدام إثبات الهوية.	اسم معلوم الهوية	Verified Name –

An entity that verifies the claimant's identity by verifying the claimant's possession of a token using an authentication protocol. To do this, the verifier may also need to validate credentials that link the token and identity and check their status. An entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges.	الجهة التي تتحقق من هوية مقدم الطلب بالتأكد من امتلاكه لإشارة السماح باستخدام أحد بروتوكولات التصديق. لعمل ذلك قد يحتاج المسؤول عن التحقق من الهوية إلى التأكد من صلاحية عناصر اعتماد المصداقية التي تربط إشارة السماح والهوية والتأكد من حالتهم. أحد الكيانات التي تكون أو تمثل الجهة التي تطلب هوية مصدق عليها. يضم المسؤول عن التحقق من صحة الهوية الوظائف الضرورية للدخول في تبادل بيانات التصديق.	المسؤول عن التحقق من الهوية	Verifier –
An attack where the attacker impersonates the verifier in an authentication protocol, usually to learn a password.	هجوم يقوم فيه المهاجم بانتحال شخصية المسؤول عن التحقق من الشخصية في أحد بروتوكولات التصديق وعادة ما يكون لمعرفة بكلمة المرور.	هجوم انتحال شخصية المسؤول عن التحقق من الهوية	Verifier Impersonation Attack –
A machine that is attacked.	الجهاز الذي جرى مهاجمته.	ضحية	Victim –
A virtual private network is a logical network that is established, at the application layer of the Open Systems Interconnection (OSI) model, over an existing physical network and typically does not include every node present on the physical network.	هي شبكة افتراضية مُنشأة في طبقة التطبيق من نموذج نظام الاتصال المفتوح فوق شبكة مادية الموجود بالفعل ولكنها عادة لا تضم كل نقاط الاتصال الموجودة في تلك الشبكة المادية.	شبكة خاصة افتراضية	Virtual Private Network (VPN) –
A self-replicating program that runs and spreads by modifying other programs or files	برنامج يقوم بنسخ نفسه ذاتياً بحيث يقوم بالعمل والانتشار عن طريق إحداث تغييرات في برامج وملفات الأخرى.	فيروس	Virus –
An urgent warning message about a nonexistent virus.	رسالة إنذار عاجل عن فيروس غير موجود.	إنذار كاذب	Virus Hoax –
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.	أوجه الضعف في نظام معلومات أو إجراءات أمن النظام أو عناصر التحكم الداخلية أو التنفيذ التي يستغلها أو يستهدفها مصدر تهديد.	ثغرة أمنية	Vulnerability –
Formal description and evaluation of the vulnerabilities in an information system.	بيان رسمي وتقييم للثغرات الأمنية في أحد أنظمة المعلومات.	تقييم الثغرات الأمنية	Vulnerability Assessment –
A term widely used by hackers to denote illegally copied and distributed commercial software from which all copy protection has been removed. Warez often contains viruses, Trojans and other malicious code and thus is very risky to download and use (legal issues notwithstanding).	مصطلح يستخدمه الهاكرز للدلالة على برامج تجارية منسوخة وموزعة بطريقة غير شرعية بعد نزع الحماية ضد النسخ عنها. عادة ما تحتوي تلك النسخ على فيروسات وأحصنة طروادة وغيرها من الشفرات الخبيثة لذلك يعد تحميل واستخدام تلك النسخ مخاطرة عالية ناهيك عن الجوانب القانونية.	نسخ غير مشروعة (ويرز)	Warez –
An environmentally conditioned workspace that is partially equipped with IT and telecommunications equipment to support relocated IT operations in the event of a significant disruption.	بيئة عمل مجهزة بشكل جزئي بمعدات تقنية المعلومات والاتصالات لدعم عمليات تقنية المعلومات المنقولة في حال وقوع خلل خطير.	موقع شبه ساخن	Warm Site –
Tiny images, invisible to a user, placed on web sites in such a way that they allow third parties to track use of web servers and collect information about the user, including IP address, Host name, browser type and version, operating system name and version, and web browser cookie.	صور دقيقة جداً لا يمكن للمستخدم ملاحظتها بالعين المجردة توضع في مواقع الويب بحيث تسمح لأطراف ثالثة تتبع استخدام خوادم الويب وجمع المعلومات عن المستخدم بما فيها عنوان بروتوكول الانترنت واسم المضيف بالإضافة إلى نوع وإصدار كلاً من المتصفح ونظام التشغيل وكذلك ملفات جمع البيانات (الكعكة) الموجودة في متصفح الويب.	منفذ الطرف الثالث	Web Bug –

Wired Equivalent Privacy, a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP was intended to provide the same level of security as that of a wired LAN.	بروتوكول أمني للشبكات المحلية اللاسلكية تم تعريفه في المعيار 802.11b بحيث يهدف إلى توفير نفس المستوى من الأمن الموجود في الشبكات المحلية السلكية .	بروتوكول الخصوصية على قنوات الاتصال اللاسلكية	Wired Equivalent Privacy (WEP) –
A standard for providing cellular telephones, pagers, and other handheld devices with secure access to e-mail and text-based Web pages	معيار يوفر لأجهزة التليفون المحمول والاستدعاء عن بعد (Pagers) وغيرها من الأجهزة الكفية المحمولة الوصول الآمن إلى صفحات البريد الالكتروني وصفحات الويب النصية .	بروتوكول التطبيقات اللاسلكية	Wireless Application Protocol (WAP) –
A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.	برنامج ينسخ نفسه وينتشر ذاتياً مستخدماً آليات التشبيك ولديه القدرة على التخفي من برامج الحماية.	دودة	Worm –
A device that allows investigators to examine media while preventing data writes from occurring on the subject media.	جهاز يسمح للمحققين القيام بفحص وسائط التخزين مع منع الكتابة على البيانات الموجودة على الوسائط الخاضعة لذلك.	مانع الكتابة على بيانات الوسائط	Write-Blocker –
The International Organization for Standardization/International Telecommunication Union – Standardization Department (ISO/ ITU-T) X.509 standard defined two types of certificates – the X.509 public key certificate, and the X.509 attribute certificate. Most commonly (including this document), an X.509 certificate refers to the X.509 public key certificate.	حسب المنظمة الدولية للقياس و اتحاد الاتصالات الدولي – قسم المعايير فان المعيار رقم X.509 يحدد نوعين من الشهادات هما شهادات X.509 للمفتاح العام وشهادات X.509 للخصائص. والأكثر شيوعاً حتى في هذا القاموس أن شهادات X.509 تشير إلى النوع الأول وهو شهادات X.509 ذات المفتاح العام.	شهادة المعيار X.509	X.509 Certificate –
The public key for a user (or device) and a name for the user (or device), together with some other information, rendered unforgeable by the digital signature of the certification authority that issued the certificate, encoded in the format defined in the ISO/ITU-T X.509 standard.	جعل المفتاح العام لأحد المستخدمين (أو الأجهزة) مقترناً باسم المستخدم (أو الجهاز) وبعض المعلومات الأخرى غير قابل للتزوير باستخدام التوقيع الرقمي الخاص بهيئة التوثيق التي تصدر الشهادة مشفرة في نسق محدد في معيار X.509 من معايير المنظمة الدولية للقياس واتحاد الاتصالات الدولي.	شهادة المعيار X.509 ذات المفتاح العام	X.509 Public Key Certificate –
A method of erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of the data.	أسلوب لإزالة البيانات المخزَّنَة الكترونياً ومفاتيح التشفير وموفري خدمة عناصر اعتماد المصداقية عن طريق تغيير أو حذف محتوي مخازن البيانات لمنع استعادتها.	التحويل للقيمة الصفرية (التصفير)	Zeroization –
A program that is installed on a system to cause it to attack other systems.	برنامج مثبت على أحد الأنظمة لكي يسخرها في مهاجمة أنظمة أخرى.	برنامج الزومبي	Zombie –