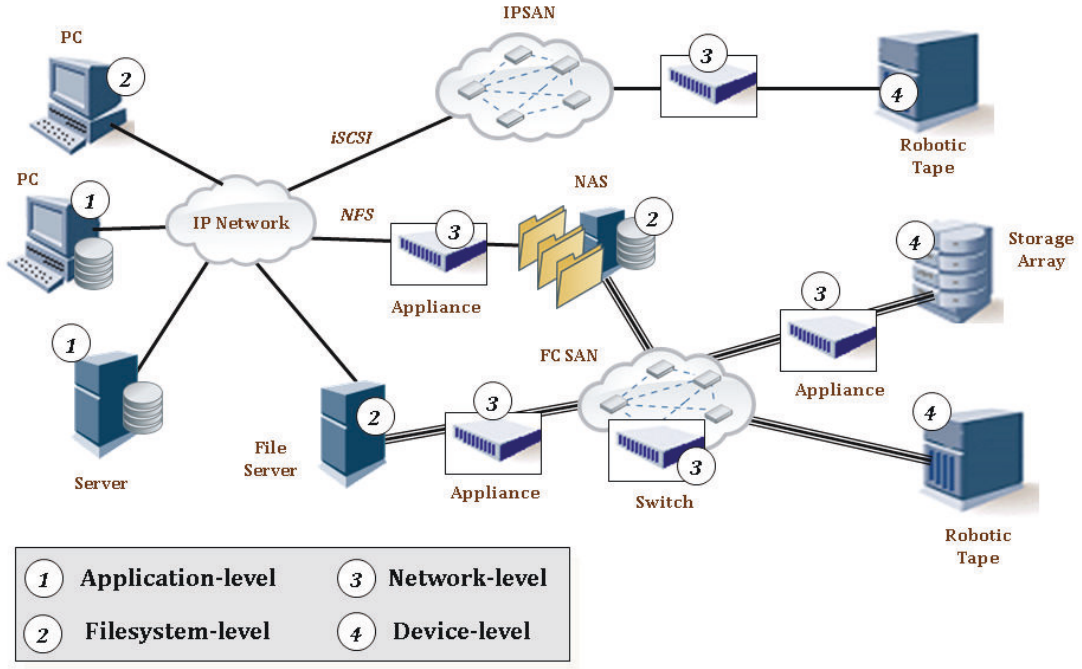

Figure 6 — Sample points of encryption

When encryption is deemed necessary, consider the following guidance:

— storage-based encryption should not be the primary form of encryption for sensitive data[24];

— selection of a point of encryption should be influenced by DR and BC (see 7.3.4), data reduction (see 6.8.3), and data protection (see 7.3.3) considerations;

— data retention (see 7.4) needs should be considered when selecting and deploying encryption;

— the security strength of the encryption solution should be at least 112 bits with 128 bits serving as the recommended minimum[25];

— cryptographic modules used to protect sensitive or regulated data should be validated using recognized criteria (e.g., ISO/IEC 19790, ISO/IEC 15408, NIST FIPS 140-2, etc.);

— multiple encryption steps can be used, as when data encrypted for privacy purposes is further encrypted by a Self-Encrypting Drive for security purposes.

As with sanitization, it is important that an organization maintain records of its data at rest encryption to document what media were protected as well as when and how they were encrypted. When an organization is suspected of losing control of its storage media, which contain sensitive information, these records or proof of encryption can be instrumental in demonstrating that no data breach

24) The storage encryption is active only while the data is resident on the storage system or media (i.e., it is plaintext once it passes through the point of encryption, which occurs any time the data is accessed).

25) Allowing for 112 bits of security strength means that Triple DES is an acceptable option, but not recommended.

occurred, thereby avoiding costly data breach notifications and other liabilities. The following should be considered for proof of encryption:

— ensure that the encryption mechanisms create appropriate audit log entries (activation, verification, integrity checks, re-keying, etc.);

— agree in advance on what audit log material demonstrates (to the satisfaction of the compliance personnel) that encryption was properly performed;

— perform regular and audited checks that encryption was properly performed and consider outside accreditation.

Successful use of cryptography is dependent on adhering to basic principles associated with keying material as well as implementing key management. As storage systems and devices integrate encryption for data at rest, key management becomes important and should address the following:

— leverage centralized key management;

— fully automate key management whenever possible;

— sparsely use keys with a long life (i.e., approaches the maximum recommended cryptoperiod, which is typically no more than 1-2 years, depending on the key type);

— enforce strict access controls to limit user capabilities and separation of duties constraints (e.g., a security role) for key generation, change and distribution;

— for sensitive or high-value data, the encryption should be end-to-end (i.e., data in motion and data at rest).

Data integrity is a significant design criterion for most storage systems and infrastructure and it is only rivalled by data availability in its importance to storage personnel. To address data integrity issues, a wide range of technologies are typically deployed in storage infrastructure, including but not limited to, RAID, backups, replications, and CDP. Although important, these data protection technologies are not typically considered part of the storage security controls.

Data retention and compliance requirements often include provisions for storing data in a manner that blocks record deletion or alteration (i.e., immutable) along with integrity verification (e.g., hashing) and explicit retention periods (e.g., legal holds) that need to be honoured. Several forms of WORM-based storage can be used to meet the immutability (non-editable) requirements. In addition, many CAS (see 6.7.3) implementations combine WORM with metadata that can be used to perform explicit integrity checks as well as enforce data expirations.

— Malware is a common threat to the integrity of data, applications, and operating system; storage systems should include sufficient malware protections to guard against attacks on data (e.g., corruption, destruction, etc.)

— WORM-based storage should be used to help meet immutability requirements

Vendors should implement the functionality for encryption, key management, and integrity described in 7.5 within their products.

7.6 Virtualization

7.6.1 Storage virtualization

Storage virtualization disconnects the logical storage abstractions used by servers and applications from the physical storage systems, devices or media on which the information is stored in a fashion that enables that logical to physical relationship to change over time and can mask the details of the physical entities. For example, a logical volume manager in a server or storage array can present portions of multiple physical disk drives as a single mirrored logical volume and be capable of rebuilding the mirrored volume to use another disk drive after a failure of one of the original drives. Another example

is that automatic tiering functionality in a storage array can change the drives on which information is stored in response to changed access patterns (e.g., move more frequently accessed information to higher performance drives).

The presence of storage virtualization is an important consideration in control design and application. Controls can be applied to logical or physical storage entities. Controls on logical storage entities are unaffected by physical relocation of the information, but controls on physical entities should be applied to the entire domain of physical entities (e.g., storage systems, devices, media) on which information subject to the control may be stored in order to avoid relocation of that information causing the control to by bypassed.

When storage virtualization can store or relocate information across a domain of distributed entities (e.g., information stored on one of multiple storage systems and relocated over time) and storage networking is in use, the appropriate storage networking controls (see 6.3) should be applied to that entire domain, as application of such a control to a subset of the domain can cause the control to be bypassed when information is relocated or new information subject to the control is stored on an entity to which the control has not been applied.

If storage virtualization exposes the physical storage entities that are virtualized (e.g., external storage virtualized by a storage array) controls should be applied to limit or prevent direct access to the non-virtualized physical elements, as such access is not equivalent to accessing the virtualized storage.

When storage is virtualized, both data sanitization controls (see 6.8.1) and data at rest encryption controls (see 6.8.2) on the physical storage entities should assume that the controlled storage entities (e.g., systems, devices and media) can contain the most sensitive information that may be stored on them. For example, if encryption is used to control the confidentiality of data stored on a disk drive that is removed from a storage array (e.g., because the drive has failed) and that storage array implements storage virtualization, then the encryption algorithm should be appropriate for protection of the most sensitive data that can be stored by the storage array.

Additional virtualization considerations include:

— ensure appropriate service level objectives for virtual storage, including:
  — match the availability objective for the storage infrastructure to the application requirements;
  — match the confidentiality and privacy requirements for the storage infrastructure to the types of information stored.
— address multi-tenancy concerns, as appropriate (see 7.7.4).

7.6.2 Storage for virtualized systems

Server virtualization extends the shared access to resources of typical operating systems to a model in which the virtualization software instead provides the illusion of more than one computer, HDD, printer, etc. The physical server typically runs a hypervisor that is tasked with creating, releasing, and managing the resources of “guest” operating systems, or Virtual Machines (VM). These guest operating systems are allocated a share of resources of the physical server, typically in a manner in which the guest is not aware of any other physical resources save for those allocated to it by the hypervisor.

When storage systems and infrastructure are used to support virtualized servers, additional care is often necessary to ensure data is available, but not unduly exposed to potential data breaches.

The following storage for virtualization guidance is relevant and should be followed:

— VM access to storage networks should be controlled via use of access controls in the server virtualization (hypervisor) software;

— N_Port_ID Virtualization (NPIV) should be leveraged appropriately to limit VM access to storage targets (see C.6 for additional information on NPIV), including:

  — configure FC SAN zones and present LUNs using the VM-specific World Wide Port Names (WWPNs), so that the LUNs will only be visible to that virtual server and not to any other virtual server;

  — avoid scaling problems due to resource limitations (e.g., state related information in servers, network fabrics, and storage) by restricting use of NPIV to creating only the N_Port_IDs that are necessary to provide isolation among larger domains (e.g., the set of VMs for a single organization or a single tenant of a service provider).

— VM migration/movement between physical servers in an infrastructure should be controlled to avoid having unintended security consequences, such as:

  — moving a VM from a lower-risk (more trusted) to a higher-risk (less trusted) domain can expose the sensitive information the server contains or allowed to process unless its configuration is hardened appropriately;

  — conversely when a VM is moved from a higher-risk (less trusted) domain to a lower-risk (more trusted) domain, its hardened configuration can interfere with normal operation unless it is matched to that appropriate for the lower-security domain;

  — VM could move to compromised virtualized servers thereby putting the data at risk.

7.7 Design and implementation considerations

7.7.1 Encryption and key management issues

The use of cryptographic technology introduces certain challenges that cannot be ignored. These challenges can include strict regulations governing the import/export of the technology as well as causing catastrophic losses under certain failure conditions.

The following encryption and key management guidance is relevant and should be followed:

— comply with import/export controls, including:

  — understand and obey government import regulations associated with encryption and key management;

  — understand and obey government export regulations associated with encryption and key management;

  — comply with corporate or government key escrow requirements; and

  — understand and obey any corporate or government requirements for making encryption keys available to corporate officials, law enforcement authorities, etc. to enable access to and recovery of encrypted data.

— plan for problems:

  — have a recovery plan in the event of a key compromise;

- have a key backup[26] plan[27] in place to ensure continued access to encrypted business/mission critical information[28].

- other problem areas
  - securely distribute key material among storage devices that process/access the same data. For example data is encrypted at one node but decrypted at a second node;
  - the effect of encryption on deduplication and compression techniques should be understood and factored in designs and implementations;
  - the inability to apply security techniques like virus scanning, etc. on encrypted data should be understood and mitigated with other mechanisms.

7.7.2 Align storage and policy

ISO/IEC 27002:2013, 5.1 states that "A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties." The presence or absence of policy plays a major role in assuring both security and compliance.

- Incorporate storage in policies
  - identify most sensitive (Personally Identifiable Information, intellectual property, trade secrets, etc.) and business/mission critical data categories as well as protection requirements;
  - integrate storage-specific policies with other policies (i.e., avoid creating a separate policy document for the storage ecosystem);
  - address data retention and protection (e.g., write-once-read-many or WORM, authenticity, access controls, etc.);
  - address data destruction and media sanitization.
- Conformance with policies
  - ensure that all elements of the storage ecosystem comply with policy (e.g., ISO/IEC 27001:2013, 5.2 and ISO/IEC 27002:2013, Clause 5);
  - give most sensitive/most critical data a priority.

7.7.3 Compliance

Complying with legal and regulatory requirements has become an important issue world-wide and this compliance is driving a significant portion of the security agenda and strategy of many organizations. In addition to the relevant compliance guidance in ISO/IEC 27002:2013, Clause 18, the following elements

---

26) Key backup is different from key escrow. Key backup is normally implemented in the context of a specific encryption/key management solution and is focused on providing the solution users (human or machine) access to the keys used to encrypt data within the solution. Key escrow can be implemented separate from an encryption/key management solution and is focused on providing third-party access (e.g. an entity who is not a user of the solution) to the keys used to encrypt data within the solution.

27) Key backup plans can take a number of forms from a simple physical copy of key material to sophisticated key management infrastructures which are designed with high availability and Disaster Recovery in mind.

28) The loss of an encryption key with no key recovery capability (backups, escrow, etc.) renders all of the corresponding ciphertext (i.e., data encrypted under the lost key) unusable. This situation and risk will persist for as long as the data is stored as ciphertext.

are key compliance aspects of storage systems and infrastructure that are of concern to an information systems (IS) auditor.

— Accountability
  — ensure that users, especially privileged users, have unique userids (i.e., no shared accounts);
  — when possible, grant rights and privileges based on roles;
  — log all attempted (successful and unsuccessful) management events and transactions.
— Traceability
  — ensure that logged event/transaction data contains sufficient application or system detail to clearly identify the source;
  — ensure that the user information can be traced to a specific individual;
  — when appropriate, treat log records as evidence[29)] (chain of custody, non-repudiation, authenticity, etc.).
— Detect, monitor, and evaluate
  — ensure that the storage layer participates in the external audit logging measures;
  — monitor the audit logging events and issue the appropriate alerts.
— Information retention and sanitization
  — implement appropriate data retention measures;
  — implement appropriate data integrity and authenticity measures;
  — correctly sanitize data upon deletion, repurposing or decommissioning of hardware;
  — correctly sanitize virtual server images, and their copies, at end of life.
— Privacy
  — implement appropriate data access control measures to control access to data and metadata (e.g., search results); assume a least privilege posture whenever possible;
  — implement appropriate data confidentiality measures to prevent unauthorized disclosure.
— Legal
  — ensure that the use of data deduplication does not conflict with data authenticity requirements;
  — ensure that data and media sanitization mechanisms do not violate preservation orders;
  — ensure that proper chain of custody procedures are followed when evidentiary data (e.g., audit logs, metadata, mirror images, point-in time copies, etc.) is handled.

NOTE Annex B can be a useful resource when auditing storage systems and infrastructure.

7.7.4 Secure multi-tenancy

Multi-tenancy, as defined by Recommendation ITU-T Y.3500 | ISO/IEC 17788:2014, focuses on the "allocation of physical and virtual resources such that multiple tenants and their computations and data are isolated from and inaccessible to one another." Secure multi-tenancy builds on this concept by adding

29) ISO/IEC 27037:2012, *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence* provides information and guidance that may be relevant when log records may serve in an evidentiary role.

security controls to explicitly guard against data breaches as well as to allow for verification of the state of these controls (e.g., they are active) and validation of the controls (i.e. assurance that they work).

When considering secure multi-tenancy, it is important to include the perspective of the tenants (including their administrators). As such, a secure multi-tenant solution needs the capability to provide secure isolation while still delivering the management and flexibility benefits of shared resources that assures:

— no tenant can determine the existence or identity of any other tenant;

— no tenant can access the data in motion (network) of any other tenant;

— no tenant can access the data at rest (storage) of any other tenant;

— no tenant can perform an operation that affects an operation performed by another tenant;

— no tenant can perform an operation that might deny service to another tenant;

— each tenant can have a configuration that is independent of other tenant's existence and configuration (For example in naming or addressing.);

— when a resource (compute, storage or network) is decommissioned from a tenant the resource should be sanitized of all data and configuration information; and

— accountability and traceability measures are available at the tenant level.

Within storage systems and infrastructure that are used in part or in whole for secure multi-tenancy solutions, the following additional security measures should be used:

— encrypted storage that is aligned with the tenants' usage of resources;

— strong symmetric encryption (i.e., minimum of 128-bits of security strength) to protect data at rest;

— secure and rapid de-provisioning (see Annex A for media sanitization, including cryptographic erase);

— trusted third-party data storage management (e.g., SNMPv3, SMI-S with TLS[30], etc.);

— automated key management providing tenant-controlled key management (leverages KMIP compliant servers);

— secure data replication (e.g., data in motion and at rest encryption);

— protect data from administrators (e.g., enforce a least privileges access model, administrators do not have access to the keying materials, etc.);

— highly available storage networking fabrics (multi-path and diverse path);

— centralized and secure audit logging (e.g., syslog over TLS);

— validation and certification (e.g., Common Criteria) of cryptographic modules and other security measures (e.g., media sanitization, access control, etc.).

Vendors should implement the functionality for secure multi-tenancy described in 7.7.4 within their products.

7.7.5 Secure autonomous data movement

Many storage systems and infrastructure have the ability to move data between different storage devices and storage elements (e.g., tiered storage), between data centres (e.g., synchronous and asynchronous data replication), to data archiving facilities, to data protection systems (e.g., backups on tape robots

30) SMI-S v1.5, which is also known as ISO/IEC 24775 *Information technology – Storage management*; is available from the Storage Networking Industry Association (SNIA). More recent versions (e.g., v1.6) are also available from the SNIA.

or virtual tape), etc. More complex scenarios exist within Information Lifecycle Management (ILM) and Data Lifecycle Management (DLM) solutions. However, all of these scenarios assume:

— data movement is policy-driven;

— intervention of operators or computers is not required to initiate or intervene throughout the process.

Because autonomous data movement takes many forms, the security needs can vary significantly; they can include some or all of the following:

— Accountability and traceability

  — configuring policies for data movement should be restricted to authenticated and authorized privileged users;

  — the individual establishing the configurations should be conversant with the security attributes of both source and destination;

  — configuration changes to implement or terminate autonomous data movement should be reflected in the audit log;

  — all autonomous data movement transactions should be reflected in the audit log of the system conducting the data movement;

— Integrity, authenticity, and immutability

  — as part of autonomous data movement transactions, the integrity of the moved data should be verified (preferably with a cryptographic hash);

  — autonomous data movement transactions should not impact the authenticity of the data (e.g., original system metadata like creation date, last accessed, etc. are correctly represented in the moved data);

  — autonomous data movement transactions should not negate immutability or other data preservation controls (e.g., supporting legal holds).

— Confidentiality

  — autonomous data movement transactions should not eliminate or weaken encryption controls associated with the data;

  — autonomous data movement transactions that span systems should include data in motion encryption for sensitive and high value data.

— Sanitization

  — as part of autonomous data movement transactions, the source data or storage media should be appropriately sanitized (see 6.8.1.2 and 6.8.1.3) before it is released for re-use;

  — sanitization performed in conjunction with autonomous data movement should also include verification (see 6.8.1.5) and some form of proof of sanitization (see 6.8.1.4).

— Trustworthiness and physical security

  — autonomous data movement transactions should not cause data to cross security domains (e.g., production to development environments);

  — autonomous data movement transactions should not cause data to move to systems with inadequate certifications and accreditations;

  — autonomous data movement transactions should not cause data to move to systems with inadequate physical security.

Vendors should implement the functionality for secure autonomous data movement described in 7.7.5 within their products.

Annex A
(normative)

Media sanitization

A.1 Methods used to sanitize media

Several different methods can be used to sanitize media with the three most common being:

— **Clear** - One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process can overwrite through the interface, or using the appropriate ATA/SCSI firmware command to overwrite both logically addressable and logically non-addressable physical media. Overwriting through the interface should include overwriting not only the logical storage location of a file (e.g., file allocation table) but also can include all addressable locations. The security goal of the overwriting process is to replace all previously written data with fixed or random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size can also influence whether overwriting is a suitable sanitization method.

— **Purge** - Degaussing, cryptographic erase (see A.3), and executing the appropriate ATA/SCSI firmware commands to use block erase operations on both logically addressable and logically non-addressable physical media are acceptable methods for purging. Degaussing is not applicable to devices that contain non-magnetic media (e.g. SSD or SSHD).

  — Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes.

  — Cryptographic Erase leverages the encryption of target data by enabling sanitization of the target data's encryption key. This leaves only the ciphertext remaining on the media, effectively sanitizing the data.

— **Destruct** - There are many different types, techniques, and procedures for media destruction. If destruction is decided on because of the high security categorization of the information, then after the destruction, the media should be able to withstand a laboratory attack.

  — *Disintegrate.* Sanitization method designed to completely destroy the media by breaking or decompose (e.g., acid) it into constituent elements, parts, or small particles.

  — *Incinerate.* Sanitization method designed to completely destroy the media by burning until it is reduced to ashes.

  — *Melt.* Sanitization method designed to completely destroy the media by liquefying it, typically through the application of heat.

  — *Pulverize.* Sanitization method designed to completely destroy the media by grinding it to a powder or dust form.

  — *Shred*. Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed.

A.2 Sanitization for different types of media

There are two primary types of media in common use:

— **Hard Copy.** Hard copy media is physical representations of information, most often associated with paper printouts. However, printer and facsimile ribbons, drums, and platens are all examples of hard copy media. The supplies associated with producing paper printouts are often the most uncontrolled. Hard copy materials containing sensitive data that leave an organization without effective sanitization expose a significant vulnerability to "dumpster divers" and overcurious employees, risking accidental disclosures. Table A.1 provides guidance for this type of media.

— **Electronic (or Soft) Copy.** Electronic media are the devices containing bits and bytes such as HDD, Random Access Memory (RAM), Read-Only Memory (ROM), disks, memory devices, phones, mobile computing devices, networking devices, office equipment, and many other types. Tables A.2, A.3, A.4, A.5, A.6, A.7, A.8, and A.9 provide guidance for common forms of electronic media.

Table A.1 — Hard Copy Storage Sanitization

Sanitization Method	Description
Paper and microforms	
Clear/Purge:	N/A, see Destruct.
Destruct:	Destruct paper using cross cut shredders that produce particles that are 1 x 5 millimetres in size (or smaller), or pulverize/disintegrate paper materials using disintegrator devices equipped with 1,5 millimetre security screen. Destruct microforms (microfilm, microfiche, or other reduced image photo negatives) by burning. When material is burned, the residue is reduced to white ash.

Table A.2 — Networking Device Sanitization

Sanitization Method	Description
Routers and Switches (home, home office, enterprise)	
Clear:	Perform a full manufacturer's reset to reset the router or switch back to its factory default settings.
Purge:	See Destruct. Most routers and switches only offer capabilities to Clear (and not Purge) the data contents. A router or switch may offer Purge capabilities, but these capabilities are specific to the hardware and firmware of the device and should be applied with caution. Refer to the device manufacturer to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destruct:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
For both Clear and (if applicable) Purge, refer to the manufacturer for additional information on the proper sanitization procedure. Network Devices may contain removable storage. The removable media should be removed and sanitized using media-specific techniques.	

Table A.3 — Mobile Device Sanitization

Sanitization Method	Description
Apple iPhone and iPad	
Clear/Purge:	Select the full sanitize option. The sanitization operation may take only minutes if cryptographic erase is supported, or may take as long as several hours if media-dependent non-cryptographic sanitization techniques that leverage overwriting are applied by the device (depending on the media size).
Destruct:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Blackberry	
Clear/Purge:	Select the full sanitize option, making sure to select all subcategories of data types for sanitization. The sanitization operation may take as long as several hours depending on the media size.
Destruct:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Devices running the Google Android operating system	
Clear:	Select the full sanitize option.
Purge:	Android settings and capabilities may be modified by device vendors or service providers, and therefore no assumptions should be made about the level of assurance provided by performing a factory data reset. Some versions of Android support encryption, and may support cryptographic erase. Refer to the device manufacturer (and potentially the service provider as well, if applicable) to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) or cryptographic erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destruct:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
All other mobile devices *This includes cell phones, smart phones, personal digital assistant, tablets, and other devices not covered in the preceding mobile categories.*	
Clear:	Manually delete all information, then perform a full manufacturer's reset to reset the mobile device to factory state.
Purge:	See Destruct. Many mobile devices only offer capabilities to Clear (and not Purge) the data contents. A mobile device may offer Purge capabilities, but these capabilities are specific to the hardware and software of the device and should be applied with caution. The device manufacturer should be referred to in order to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) or cryptographic erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destruct:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Disassembly of battery and display may be required. Following the Clear or (if applicable) Purge operation, manually navigate to multiple areas of the device (such as call history, browser history, files, photos, etc.) to verify that no personal information has been retained on the device. For both Clear and (if applicable) Purge, refer to the manufacturer for proper sanitization procedure. Refer to the manufacturer for additional information on the proper sanitization procedure, and for details about implementation differences between device versions and operating system versions. Proper initial configuration using guides helps ensure that the level of data protection and sanitization assurance is as robust as possible. If the device contains removable storage media, ensure that the media is sanitized using appropriate media-dependent procedures.	