**STATE of ARIZONA – Government Information Technology Agency**

| | | |
|---|---|---|
| **S**tatewide **I**nformation **S**ecurity and **P**rivacy **O**ffice | **SISPO STANDARD** | **TITLE:** **Incident Submission and Response** |
| | **P900-S905** | **Effective Date: May 31, 2011** |

## 1. AUTHORITY

Under the authority of A.R.S. § 41-3507 and Executive Order 2008-10, The Statewide Information Security and Privacy Office (SISPO) is responsible for ensuring development and implementation of risk mitigation strategies by each budget unit to identify threats and vulnerabilities to the confidentiality, integrity and availability of state information and the information technology infrastructure.

## 2. PURPOSE

This standard identifies the minimum elements a budget unit shall implement and maintain to provide for the prompt identification, reporting, management and resolution of an information security incident as defined by the GITA SISPO Information Security Incident Policy, P900.

## 3. SCOPE

This standard applies to all budget units whose workforce or contractors are authorized to access or use the state information technology infrastructure or who access, use or disclose state information at any location where the activity is performed. State information includes any format or on any medium (e.g. electronic, hardcopy, and records generally as defined by A.R.S. § 41-1350) including oral communications.

## 4. STANDARD

### 4.1. DEFINITIONS

4.1.1 "AZNet" means the contractor for the State of Arizona telecommunications and network.

4.1.2 "Budget unit" means a department, commission, board, institution or other budget unit of the state organization receiving, expending, or disbursing state funds or incurring obligations of the state including the Arizona Board of Regents but excluding the universities under the jurisdiction of the Arizona Board of Regents, the community college districts and the legislative or judicial branches. A.R.S. § 41-3501(2).

4.1.3 "Chief Executive Officer" (CEO) means the chief executive officer of a budget unit (See also GITA Administrative Rule. R2-18-101(2)).

4.1.4 "Confidential Information" (CI) means information other than Restricted Personal Identifying Information (RPII) that may only be disclosed as permitted or required by state or federal law or administrative rule. Confidential information includes critical business infrastructure information as defined by ARS 41-1801 and critical infrastructure information as defined by the U.S. Department of Homeland Security (6 USC 131; 49 CFR 1520).

4.1.5 "Contractor" means an individual, government entity or non-government business entity providing products or services for a budget unit or on behalf of a budget unit. The term "contractor" includes a "business associate" as defined by HIPAA at 45 CFR 160-103 [insert hyperlink], temporary personnel or other third parties, including subcontractors or other agents utilized by a contractor, that are not part of the budget unit workforce but have access Restricted Personal Identifying Information (RPII), confidential or sensitive information or to the state information technology infrastructure.

4.1.6 "Data Breach" means an information security incident involving (1) unauthorized access of Restricted Personal Identifying Information (RPII) and (2) the unauthorized access poses a substantial risk of financial, reputational or other harm to individuals affected by the incident. (See the Notification of Breach of Security System, the Arizona data breach notification law, ARS 44-7501 and the Health Insurance Portability and Accountability Act (HIPAA) data breach notification standard, 45 CFR Part 164, Subpart D).

4.1.7 "Discovery" means the date and/or time a budget unitor contractor becomes aware of or reasonably believes an information security incident has occurred.

4.1.8 "Information Privacy Incident" means an information security incident resulting in unauthorized access of personal identifying information defined by this policy as Restricted Personal Identifiable Information (RPII), Confidential Information (CI) or Sensitive Information (SI).

4.1.9 "Information Security Incident" or "Incident" means an event, as referenced in ARS 41-3507(E), that a budget unit, a budget unit's or contractor, or the state reasonably believes has the potential to compromise the confidentiality, integrity, or availability of a RPII, CI or SI or the state information technology infrastructure.

4.1.10 "Restricted Personal Identifying Information" (RPII) means data elements that are a subset of confidential information and create a high severity risk information security incident from unauthorized access. The RPII also may be subject to the Arizona data breach notification law (ARS 44-7501) or HIPAA data breach notification standard (45 CFR Part 164, Subpart D). The data elements defined as RPII by this policy are:

(a) An individual's first name or first initial and last name in combination with any one or more of the following data elements for the individual, when the data element is not encrypted, redacted or secured by any other method rendering the information unreadable, unusable or undecipherable:

- Social security number
- Driver license number
- Non-operating identification license number
- Financial account number, credit card number, debit card number, or charge card account number
- Financial account number, credit, debit, or charge card account number in combination with computer access information as defined by ARS 13-2301(E)(2), including any security code, access code, biometric identifier or record, password or user ID for access to any electronic file or account

(b) "Protected Health Information" (PHI) as defined by the Privacy Rule of the Health Insurance Portability and Accountability Act or 19961 (HIPAA) as maintained by a budget unit that must comply with HIPAA.[i]

4.1.11 "Sensitive Information" (SI) means personal identifying information or other categories of information that if disclosed are reasonably likely to adversely affect the best interest of the state or the best interest of an individual. SI may include personal identifying information as discussed in the Arizona statute Government Anti-Identification Procedures (ARS 41-4171 and 41-4172) when such information is not otherwise defined as "restricted personal identifying information" or "confidential information.

4.1.12 "Unauthorized Access" means to access, acquire, use, disclose, view, exchange, transmit, maintain, retain, modify, store, record, dispose of or destroy RPII, CI or SI without authority, in excess of authority or with the intent to compromise the confidentiality of the information. Unauthorized Access includes the loss or other unauthorized access of a device, technology component or record containing RPII, CI or SI or the

destruction/disposal of records that does not comply with the Arizona Record Destruction law, ARS 44-7601.

## 4.2. INFORMATION SECURITY INCIDENTS

4.2.1. This standard addresses submission and response to information security incidents that affect the state information technology infrastructure, components of that infrastructure and devices that interface with the state information technology infrastructure.

4.2.2. The standard includes submission and response to information security incidents that involve unauthorized access to RPII, CI or SI and that compromise the confidentiality of such information. These incidents are also called "information privacy incidents."

## 4.3. SEVERITY CATEGORY

4.3.1. The budget unit shall use "high", "medium" or "low" to categorize the level of severity for a technology or non-technology incident:

(a) **High** -- an incident that will or is reasonably likely to have a **substantial, material, significant or catastrophic adverse effect** on budget unit operations, state information technology infrastructure, the privacy of individual by unauthorized access to RPII, or the best interest of the state. A budget unit shall report a high risk severity incident to the SISPO incident system within **one (1) business day** after discovery of the incident. For examples of high severity incidents see Appendix A.

(b) **Medium** -- an incident that will or is reasonably likely to have a **serious adverse effect o**n budget unit operations, state information technology infrastructure, or the privacy of individual by unauthorized access to CI or SI. A medium risk severity incident shall be reported within **two (2) business days** after discovery of the incident. For examples of medium severity incidents see Appendix A.

(c) **Low** -- an incident that will or is reasonably likely to have a **limited adverse effect** on budget unit operations, assets, or individuals. The event could be expected to cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs. A low risk incident shall be reported to the SISPO incident report system within **five (5) business days** after discovery of the incident. For examples of low severity incidents see Appendix A.

## 4.4. TECHNOLOGY INFRASTRUCTURE -- INFORMATION SECURITY INCIDENT

4.4.1. Each budget unit shall participate with AZNet, the State Information Protection Center (SIPC) and SISPO to identify, report after discovery, and respond to all information security incidents.

4.4.2. Upon discovery of a technology related incident, a budget unit will evaluate the severity of the incident and categorize as high, medium, or low as described in section 4.3.

4.4.3. If the incident is categorized as high severity, a budget unit shall provide initial notification to SIPC within one (1) hour of discovery using email or phone. The budget unit's initial notification shall include:

(a) The budget unit's Information Security Officer's name, phone number and email address

(b) Budget unit name and physical location

(c) Date and time incident detected

(d) Ability to conduct core business functions

(e) Brief description of intrusion and damages (real or anticipated)

(f) Unauthorized access of RPII, CI or SI

4.4.4. The budget unit will additionally submit an incident report to the IRR system in a time frame consistent with the severity category in section 4.3.

4.4.5. If the incident is categorized as medium severity (i.e. AZNet non-critical alerts), a budget unit will submit an incident report consistent with section 4.3.

4.4.6. If the incident is categorized as low severity (i.e. AZNet possible non-essential network traffic alerts), a budget unit will submit an incident report consistent with section 4.3.

## 4.5. AZNet ALERT NOTIFICATION -- TECHOLOGY INFRASTRUCTURE INCIDENT

4.5.1. AZNet, in collaboration with SIPC and SISPO, will notify a budget unit within **one (1)** hour of discovery of a threat or vulnerability to the budget unit's technology infrastructure. A budget unit must respond to the

AZNet alert notification according to the AZNet-determined events described below:

(a) **Critical Alert – Reply with One (1) Hour to AZNet**

(i) A Critical Alert means AZNet has detected suspicious activity related to the budget unit's information technology infrastructure that poses a high probability of a high severity risk to the budget unit and/or to the state's information technology infrastructure. See Appendix B for this type of incident.

(ii) A budget unit will confirm the threat within one hour after alert receipt and indicate the steps it is taking to contain the threat or vulnerability including, if indicated, shut down the infected part of the budget unit technology infrastructure. A Critical Alert that becomes a confirmed incident is classified as "high severity" and requires submission of an incident report to the IRR system (see section 4.3).

(iii) Failure to respond to AZNet within one (1) hour or take immediate containment action may result in AZNet's temporary suspension of the budget unit's technology infrastructure.[ii]

(iv) The budget unit shall not resume technology operations until AZNet confirms the threat or vulnerability is contained and poses no further harm.

(b) **Non-Critical Alert**. **– Reply to SIPC within Two (2) Days**

(i) A Non-Critical Alert means AZNet has detected suspicious activity that requires the budget unit to confirm the severity of the activity and if the nature is either a) a "false positive" and is business related, or b) an event that will not critically impact the budget unit or the state technology infrastructure. See Appendix B for this type of incident.

(ii) The budget unit will categorize the severity of the incident according to the nature of the event, the resources impacted, and the resources required to remediate. The budget unit will submit an incident

report according to the level of severity and consistent with section 4.3.

(c) **Possible Non-essential Network Traffic – Reply to SIPC within Five (5) Days**

(i) Possible Non-essential Network Traffic means AzNet detects a high volume of network traffic going to or coming from a budget unit that appears not have a business related purpose. A budget unit must investigate the activity and assist SIPC and AZNet to alleviate the burdensome impact to the state shared information technology network. See Appendix B for examples of this type of incident.

(ii) A budget unit must respond to a Non-essential Network Traffic alert by notifying SIPC as soon as possible but within five (5) business days. A budget unit whose business related network traffic over-burdens the state shared network must assist SIPC, AZNet and SISPO to alleviate the threat to the state information technology system.

(iii) The budget unit will implement system and authorized use controls to mitigate future occurrences of the same or similar activity.

(iv) The budget unit will submit an incident report to the IRR system as a "low severity" event within five (5) business days (see section 4.3).

## 4.6. INFORMATION PRIVACY INCIDENTS

4.6.1. Information security incidents that involve unauthorized access to RPII are "information privacy incidents." All information privacy incidents shall be reported to SISPO using the IRR system or the alternative method of submission (see section 4.7.2) by the budget unit ISO, APO or HCO. Privacy incidents include compliance violation with data safeguards required by federal laws (other than HIPAA), regulations and industry standards [iii] or unauthorized access to HIPAA defined protected health information (see 45 CFR 160.103). For examples of information security incidents that are also privacy incidents see Appendix A.

4.6.2. All information privacy incidents shall be submitted and classified consistent with section 4.6 of this standard. The report shall identify as specific as possible what RPII, CI or SI was affected by the incident.

4.6.3. Unauthorized access to RPII is always a ”high severity” event that requires a prompt risk assessment to determine if affected individuals must be notified of the data breach (refer to the SISPO Data Breach Notification Standard, P900-S910, Section 4.4).

4.6.4. A budget unit shall notify its contractors who may be affected by an information privacy incident.

## 4.7. INCIDENT REPORT SUBMISSION

4.7.1. A budget until shall submit an incident report for each actual or suspected information security incident. The risk severity level (refer to section 4.3) determines the time frame for submission of an incident report.

4.7.2. The electronic SISPO Incident Report and Response (IRR) system will be used by state budget units to submit an information security incident report. The IRR System and data base are administered by the State Information Security and Privacy Office (SISPO) and the ADOA State Information Protection Center (SIPC) for the submission, management and trending of state information security incidents. If the SISPO IRR system is not available, the budget unit shall complete the online SISPO incident report form found at http://www.azgita.gov/sispo/notification.htm. Alternatively, the budget unit may contact SIPC (SIPC@azdoa.gov) or SISPO (SISPO@azgita.gov) to report an incident.

4.7.3. Incident reports shall contain at minimum the following information:

(a) Date the incident occurred if known; if unknown, the date the incident was discovered

(b) Incident “Type” (General and HIPAA) and “Subtype” (e.g. theft, loss, unauthorized access)

(c) Incident risk severity level (e.g. high, medium, or low), see section 4.3.

(d) Impact to a Confidential Data Asset (not PII) or PII (i.e. RPII, CI or SI)

(e) Impact to integrity or availability of information or to a critical business function

(f) Encryption of data or device involved

(g) Number of records or files and individuals impacted

(h) Whether the incident is a "data breach" (if known at time of submission or update when known)

(i) The steps taken to investigate, remediate and close the incident

(j) Any other information that may be relevant to determining the severity, mitigation or remediation of the incident

4.7.4. A completed incident report will provide sufficient detail (e.g. completion of applicable data fields) to describe the incident and the incident remediation in a factual, objective manner. The comments section will be used for brief updates and to specify what data elements are involved in the incident. Longer narratives relevant to the incident investigation and remediation may be "attached" to the electronic report (e.g. incident summary, exhibits or notification letters).

4.7.5. The budget unit shall update the incident report every 14 days or more frequently as information becomes available and consistent with section 4.10 until incident closure (i.e. as soon as possible but within **60 days** after discovery of the incident).

## 4.8. INCIDENT INVESTIGATION

4.8.1. The APO or HCO shall promptly initiate and facilitate the incident investigation utilizing the budget unit's incident response team (see SISPO Incident Security Incident Management Policy, section 4.3.5).

4.8.2. The investigation will at minimum include the following information about the incident:

(a) Nature and scope of the event

(b) Severity level (high, medium, low), see section 4. 3

(c) Ability to contain or reduce risk of harm (e.g. recover the information or device)

(d) Number of individuals affected

(e) Resources needed to promptly complete the incident investigation and contain damage and/or risk of damage

(f) Other steps to effectively manage risk reduction and incident resolution

4.8.3. When an incident is a potential/actual data breach, the budget unit investigation will also be consistent with the Data Breach Notification Standard, P900-S910.

4.8.4. Whenever possible, the budget unit should capture and maintain log entries for a minimum of one (1) week following the detection of intrusion or longer dependent on the severity of the incident or as needed to investigate the incident or to determine its root cause. Log entries provide significant detail that can be used for investigation and prosecution of the intruder.

## 4.9. INCIDENT INVOLVING MULTIPLE BUDGET UNITS

4.9.1. SISPO shall be notified by a budget unit when an information security incident involves or is likely to involve multiple budget units. Each budget unit is responsible to submit an IRR system incident report for the incident events that pertain to the budget unit. The report will be updated periodically following the timeframes discussed in section 4.10 until incident closure.

4.9.2. AZNet and/or SIPC will alert all budget units that may be affected by an information technology security incident. Each budget unit is responsible for responding to AZNet or SIPC as discussed in section 4.5.

4.9.3. SISPO shall facilitate and budget units will participate in a multi-budget unit workgroup to coordinate incident management including incident investigation and mitigation, communication with state and budget unit leadership, preparation of media releases and public notification as may be indicated by the severity of the incident.

4.9.4. SISPO, the Government Information Technology Agency Director of Communications and public information officers of the affected budget units shall develop and implement a coordinated response plan if publication or disclosure to the media is advised or required because incident severity (refer to SISPO Data Breach Notification Standard, P900-S910, section 4.7).

## 4.10. INCIDENT RESPONSE AND CLOSURE

4.10.1. A budget unit shall update an incident in the IRR System as new information becomes available until the incident is closed. The incident stage (i.e., new, investigation, mitigation or closed) must be advanced every **14 days until incident closure at 60 days after incident discovery** unless the budget unit notifies SISPO of a delay due to a criminal investigation or other complicating factor (e.g., multiple budget units, complex contractor investigation). After notifying SISPO, the budget unit

will record the cause for the delay in the "comments" section or save as an "attachment" to the IRR system report.

4.10.2. For high and medium severity incidents, a budget unit will provide an update **30** days after the date of incident discovery on the status of remediation and anticipated incident closure date. The **30 day report** may be combined with the second 14 day status update. If the incident is believed to be a data breach, the report will include:

(a) Results of the risk assessment (see Data Breach Notification Standard, section 4.4)

(b) Anticipated method of notification of individuals, if required

(c) Anticipated date of notification and incident closure

4.10.3. The budget unit must complete and provide to SISPO its final incident remediation and corrective action plan no later than **60 days after the date of incident discovery** unless there is a delay because of criminal investigation or other complication for response and closure of an incident (see Incident Submission and Response Standard, section 4.10).

## 5. CONTRACTOR RESPONSIBILITIES

5.1 The budget unit will execute a data exchange/use agreement consistent with the Government Information Technology Classification and Categorization of Data Standard P740-S741, section 4.7. The agreement will identify what specific data elements of RPII, CI or SI will be exchanged or used during the course of the agreement. Refer to the Data Matrix, P900-E901, Exhibit 1 for examples of data elements that are defined by SISPO policy as RPII, CI, or SI.

5.2 All agreements with contractors that permit access to the state information technology infrastructure or access to RPII, CI or SI shall require full collaboration and cooperation with the budget unit for the prompt discovery, mitigation, and closure of incidents.

5.3 Expected collaboration with the budget unit by the contractor should include:

(a) Who the contractor must contact at a budget unit to report an information security incident

(b) Time frame for notification of incident (see severity category section 4.3)

(c) Specific information about the nature of incident, services impacted and individuals affected including:

- The number of files, records or persons affected
- Contact information for persons affected
- Whether the information was recovered, could not be retained or otherwise used or further disclosed by the unauthorized recipient
- Encryption of the information or device affected
- Circumstances which render the information unusable, unreadable or indecipherable and cannot be re-identified (e.g. redaction, destruction)
- Other assistance the budget unit may request to assess risk of harm, notify individuals, plan and implement corrective action, report to an enforcement entity or otherwise remediate and close the incident.

5.4 The budget unit should conduct periodic written assessments to determine that its contractors comply with the budget unit or State Procurement Office contractor provisions pertaining to this Standard.

## 6. CORRECTION ACTION AND ENFORCMENT

The need for corrective action and enforcement will be factors considered for mitigation of the incident and for determining the root cause of the incident (see Information Security Incident Management Policy, Section 5).

## 7. RETENTION OF RECORDS

See Incident Security Incident Management Policy, section 6.

## 8. AUTHORITIES

- ARS 41-3507 – Duties, Statewide Information Security and Privacy Office
- Executive Order 2008-10 – Executive Order, Mitigating Cyber Threats
- ARS 41-3504 – Powers and Duties of the Agency
- ARS 44-7501 – Notification of Breach of Security System (AZ Data Breach Law)
- 45 CFR Parts 160, 162 and 164 – Rules for the Health Insurance Portability and Accountability Act of 1996 and as amendment by the Health Information Technology for Clinical and Economic Health Act, 2009
- GITA Statewide Policy P740-S741, Classification and Categorization of Data Standard

---

[i] References to HIPAA mean the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") as amended b the American Recovery and Reinvestment Act of 2009 (Pub. L No. 111-5) (the "HITECH Act") any associated regulations and the federal regulations published at 45 CFR Parts 160 and 164 (collectively referred to as "HIPAA").

[ii] Delegation of authority by GITA/SISPO to AZNet for implementation of ARS 41-3507(D) is pursuant to GITA – ADOA Memorandum of Understanding: AZNet Critical

Incident – Temporary Shutdown of State Network Infrastructure Services Criteria, dated October 27 2009.

[iii] Examples of such laws, regulations or industry standards include but are not limited to the Federal Trade Commission Health Breach Notification Rules (a breach of unsecured Personal Health Records, as required by 16 CFR 318), the Payment Card Industry (PCI) Data Standards (protection of payment card information) and the Financial Services Modernization Act of 1999 (also known as the "Gramm Leach Bliley Act" which safeguards financial information held by "financial institutions" as defined by Act).

## Appendix A
## SISPO Incident Submission and Response Standard

### TABLE OF PRIVACY INCIDENT TYPES

| SEVERITY OF INCIDENT – PRIVACY – DATA/RECORDS IMPACTED | | |
|---|---|---|
| **HIGH** | **MEDIUM** | **LOW** |
| **Unauthorized access to RPII** whether or not classified as a data breach such as:<br>--accidental or unauthorized transmission of RPII to another budget unit, contractor or unaffiliated third party<br>--improper disposal of RPII<br>--unauthorized communication of RPII | | |
| Loss, theft or other unauthorized access of a Personal Digital Assistant (PDA), smart phone, mobile device or flash drive containing RPII | Loss, theft or other unauthorized access of a Personal Digital Assistant (PDA), smart phone, mobile device or flash drive containing CI or SI with medium severity risk | Loss, theft or other unauthorized access of a Personal Digital Assistant (PDA), smart phone, mobile device or flash drive containing CI or SI with low severity risk |
| **Unauthorized access to CI or SI** and risk assessment indicates high severity risk to individuals or the state | **Unauthorized access to CI**; incident violates an Arizona statute but does not have the potential to harm individuals or the state | **Unauthorized access to SI** and incident does not have the potential to harm individuals or the state |

| HIGH | MEDIUM | LOW |
|---|---|---|
| Loss or theft of RPII during transit, such as packages that are lost or misdelivered | Loss, theft or other unauthorized access of CI during transit, such as packages that are lost or misdelivered unless a high severity risk | Loss, theft or other unauthorized access of SI during transit, such as packages that are lost or misdelivered unless a moderate or high severity risk |
| Unauthorized oral communications of RPII | Incidents pertaining to compliance with data safeguards as required by other federal laws, regulations and industry standards | |
| Loss, theft or other unauthorized access to records (hard cop Loss, theft or other unauthorized access of physical IT assets including computers, storage devices (such as flash drives), or storage media (such as CDs) that contain RPII, CI or SI y or electronic) containing RPII | Loss, theft or other unauthorized access to records (hard cop Loss, theft or other unauthorized access of physical IT assets including computers, storage devices (such as flash drives), or storage media (such as CDs) that contains CI if medium severity risk | Loss, theft or other unauthorized access to records (hard cop Loss, theft or other unauthorized access of physical IT assets including computers, storage devices (such as flash drives), or storage media (such as CDs) that contains SI if low severity risk |
| Unauthorized access to records or technology infrastructure/device resulting in consumer fraud or the potential to cause ID Theft (see also Arizona Computer Tampering Law, ARS 13-2316) | | |
| A violation of the Health Insurance Portability and Accountability Act (HIPAA) privacy standard policies related to the rules required for safeguarding of protected health information (PHI) | | |

## Appendix B
## SISPO Incident Submission and Response Standard

### TABLE OF TECHNOLOGY INCIDENT TYPES

| SEVERITY OF INCIDENT – TECHNOLOGY INFRASTRUCTURE OR DEVICE IMPACTED | | |
|---|---|---|
| **HIGH** | **MEDIUM** | **LOW** |
| An event that compromises the confidentiality, integrity, or availability of RPII (see Privacy Severity Table) | Unauthorized access to an IT device (server, storage, or client) or network without impact to confidentiality, integrity or availability of data or device | A threat or vulnerability that is quickly contained without replacement of a device, application or restricted use of the network (low risk severity). |
| Denial of service (DOS) attack | A SQL injection disables a website but does not result in unauthorized access to state information (medium risk severity). | |
| Unauthorized access that alters, damages, or destroys any IT device, network, or any physically or logically connected IT devices or any computer application systems, programs, or data | A threat or vulnerability that interrupts the budget unit's information technology infrastructure, does not impede the budget unit's activities or create a significant harm but requires moderate mitigation (e.g. device or application replacement; part of network closed off) (medium risk severity). | |

| HIGH | MEDIUM | LOW |
|---|---|---|
| Intentional disruption of any services provided through the use of any IT device or network or other violation of the Arizona computer tampering law (ARS 13-2316) | | |
| Multiple attempts to access an IT device or network system within a brief period of time for purposes of creating a threat or vulnerability to the confidentiality, integrity or availability of a technology infrastructure | | |
| Introduction of a computer-related contaminant (e.g., malicious code, virus, worm, etc.) into any IT device or network | | |