Federal Cyber Incident and Breach Reporting

This chart endeavors to track all existing and proposed cyber incident and data breach reporting requirements issued by the U.S. federal government. It is subject to change as new requirements are issued or modified.

Please note: this chart is for research purposes only and should not be interpreted as legal advice.

For questions, please contact Mary Brooks (mbrooks@rstreet.org) or Sofia Lesmes (slesmes@rstreet.org).

Acronym Key

Abbreviation	Full Name
BSA	Bank Secrecy Act
CFATS	Chemical Facility Anti-Terrorism Standards
CIA	Central Intelligence Agency
CISA	Cybersecurity and Infrastructure Security Agency
CPNI	Customer Proprietary Network Information
CRG	Cyber Response Group
CSIRT	Computer Security Incident Response Team
DCSA	Defense Counterintelligence and Security Agency
DFARS	Defense Federal Acquisition Regulation Supplement
DFS	Department of Financial Services
DHS	Department of Homeland Security
DoD	Department of Defense
DoE	Department of Energy
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FDIC	Federal Deposit Insurance Corporation
FERC	Federal Energy Regulatory Commission
FinCEN	Financial Crimes Enforcement Network
FISMA	Federal Information Security Management Act
FTC	Federal Trade Commission
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
ICT	Information and Communications Technology
MTSA	Maritime Transportation Security Act
NCCIC	National Cybersecurity and Communications Integration Center
NERC	North American Electric Reliability Corporation
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
NSC	National Security Council
NY DFS	New York Department of Financial Services
OCC	Office of the Comptroller of the Currency
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OTS	Office of Thrift Supervision
PHI	Protected Health Information
PHR	Personal Health Records
SEC	Securities and Exchange Commission
SOC	Security Operations Center
TSA	Transportation Security Administration

Name of Regulation or Other Implementing Framework	Lead Implementing Entity	Key Authorizing Mechanism or Authority; Supplementary Authorities as Applicable	Year Regulation Issued or Effective; Others as Applicable	Scope or Intent of Rule	Private or Public Disclosure	Threshhold for Disclosure	Timeline for Disclosure
Title Pending—Rulemaking pursuant to the **Cyber Incident Reporting for Critical Infrastructure Act of 2022**	**CISA**	**Cyber Incident Reporting for Critical Infrastructure Act of 2022** (Public Law No: 117-103 (Division Y))	Proposed rulemaking required: **2024**	**Cyber incident reporting:** To require covered critical infrastructure entities (list to be defined by CISA) to report a covered cyber incident to CISA; also to require covered entitites to report a ransomware payment to CISA. Non-covered entities can voluntarily report cyber incidents and ransomware payments to CISA.	Private disclosure to CISA. Liability and anonymization protections are written into the bill.	Unknown. CISA has two years to issue a proposed rulemaking governing the process, and another year and a half to issue the final rule.	In the first instance of reporting on covered events, the deadline is 72 hours from discovery of the incident. In the second instance of ransomware payments, the timeline is 24 hours from the payment.
CISA Federal Incident Notification Requirements (US-CERT Federal Incident Notification Guidelines)	**CISA / CISA Central**	**Federal Information Security Modernization Act of 2014** (44 U.S.C. 3553-54) Also routinely updated by White House memoranda, the most recent of which is available here.	Law passed: **2014** Effective: **2017**	**Cyber incident reporting:** To require federal civilian executive branch agencies to promptly disclose cybersecurity incidents and provide notification to Congress of major incidents.	Generally, private disclosure to CISA and the OMB; however, it is generally included in annual congressional FISMA metrics reporting by CISA and OMB. Note that "major" incidents must be reported to Congress.	In general: "information security incidents, where the confidentiality, integrity, or availability of a federal information system of a civilian Executive Branch agency is potentially compromised." For "major incidents," severity is determined by impacted agency, in consultation with CISA.	For most incidents: "Within one hour of being identified by the agency's top-level CSIRT, SOC, or information technology department." For major incidents: Report to Congress within seven days.
Risk-Based Performance Standards (RBPS) 15—Reporting of Significant Security Incidents	**CISA / CISA Central**	**Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014** (6 U.S.C. § 621, et seq.)	Updated: **2009** (Cyber incident reporting guidance under CFATS RBPS 8)	**Cyber Incident Reporting:** To require facilities under the Chemical Facility Anti-Terrorism Standards (CFATS) program to establish protocols to report significant cyber incidents.	Generally, private disclosure to CISA. Depending on the security program, to local and federal law enforcement.	A "significant" incident as defined by each covered facility's incident response program.	Unclear from text.
CG-5P Policy Letter 08-16, Reporting Suspicious Activity and Breaches of Security	**Coast Guard**	Issued within agency rulemaking authority under the **Maritime Transportation Security Act** (46 U.S.C. 701)	Issued: **2016** Additional Guidance: **2020** (NVIC 01-20)	**Cyber incident reporting:** To require Maritime Transportation Security Act (MTSA)-regulated vessels and facilities to report on events that may result in a transportation security incident, including breaches of security or suspicious activity.	Private disclosure to the National Response Center. Exclusively cyber incidents (with no physical component) can be reported to CISA Central.	Generally, "vessel and facility operators shall use their best judgment in making reports." Events should be reported when "security measures have been circumvented, eluded, or violated" or are "out of the ordinary."	Per 33 CFR part 101.305 (b): "without delay."

Name of Regulation or Other Implementing Framework	Lead Implementing Entity	Key Authorizing Mechanism or Authority; Supplementary Authorities as Applicable	Year Regulation Issued or Effective; Others as Applicable	Scope or Intent of Rule	Private or Public Disclosure	Threshhold for Disclosure	Timeline for Disclosure
Defense Federal Acquisition Regulation Supplement **(DFARS) Clause 252.204-7012:** Safeguarding Covered Defense Information and Cyber Incident Reporting	**DoD**	In part, 10 U.S.C. 2545 and 50 U.S.C. 3043 and in accordance with 41 U.S.C. 1304 *Note, DFARS is a mix of law, DoD policies, delegations of FAR authorities, and more. For more, see link.	Effective: **2017** CMMC Proposed: **2020** CMMC 2.0 Proposed: **2021**	**Cyber incident reporting:** To require contractors for the DoD—including subcontractors—to report cyber incidents against "covered defense information" and/or "covered contractor information systems" to the DoD.	Private disclosure to DoD.	"...when a Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support..."	"Rapidly," defined as within 72 hours of discovery.
Defense Federal Acquisition Regulation Supplement **(DFARS) Clause 252.239-7010:** Cloud Computing Services	**DoD**	In part, 10 U.S.C 2545 and 50 U.S.C. 3043, and in accordance with 41 U.S.C. 1304. *Note, DFARS is a mix of law, DoD policies, delegations of FAR authorities, and more. For more, see link.	Issued: **2016**	**Cyber incident reporting:** To require contractors who provide cloud-computing services to the DoD or who use cloud-computing services in their work to report "all cyber incidents that are related to the cloud computing service provided" to the DoD under contract.	Private disclosure to DoD.	"... all cyber incidents that are related to the cloud-computing service provided under [a relevant] contract."	Unclear from text.
Cyber Incident Handling Program (DoD 8530.01)	**DoD**	**DoD Directive 5144.02** (in turn, issued under the authority given to the Secretary of Defense under 10 U.S.C. 113)	Original: **2012** Update: **2017**	**Cyber incident reporting:** To ensure that DoD components report unauthorized or anomalous activity on DoD information networks.	Private disclosure to "DoD Component defense criminal investigative organizations; law enforcement organizations; and the IG DoD." If cleared defense contractors are involved, DCSA is also notified.	"all suspicious activity on DoD information networks and [information systems]."	Variable depending on severity. See "Table C-A-1. Reporting Timelines" available here.

Name of Regulation or Other Implementing Framework	Lead Implementing Entity	Key Authorizing Mechanism or Authority; Supplementary Authorities as Applicable	Year Regulation Issued or Effective; Others as Applicable	Scope or Intent of Rule	Private or Public Disclosure	Threshhold for Disclosure	Timeline for Disclosure
Form OE-417: Department of Energy Electric Emergency Incident and Disturbance Report	**DoE**	**Federal Energy Administration - Administrator's Information - Gathering Power** (15 U.S.C. 772(b)) *Note that entities reporting to NERC can substitute Form OE-417 for CIP-008-6.	Cyber-specific reporting as of: **2012** Update: **2018** Revisions proposed: **2020**	**Cyber incident reporting:** To require specified electric utilities to report to the DoE over "electric emergency incidents and disturbances" and enable them "to investigate significant interruptions of electric power or threats to the electric system reliability."	Private disclosure to the DoE, but high-level summaries are published in a public data table.	Variable, depending on severity. Note that cybersecurity events are only one type of threat reported on Form OE-417. A description of different thresholds is available in the form instructions.	Variable. Depending on severity, reporting may be required "within one hour; six hours; by the end of the next calendar day after a determination of an attempted cyber compromise; or by the later of 24 hours after the recognition of the incident OR by the end of the next business day of the incident."
Title Pending— Currently listed as **FAR 2021-017 - Cyber Threat and Incident Reporting and Information Sharing** (text not yet public; see reference here)	**FAR Council**	FAR was established in part by a 1979 statute. For more, see here. More recently, the Biden-era **Executive Order on Improving the Nation's Cybersecurity (EO 14028)** ordered the FAR council to update its cybersecurity incident reporting rules.	Update expected: **2022**	**Cyber incident reporting:** To require ICT service providers who enter into contracts with federal civilian executive branch agencies to report cybersecurity compromises to said affected agencies and to CISA.	Private disclosure to impacted agencies; also to CISA.	Unknown. Text of proposed rulemaking is not yet public. Policy language in the executive order states the following: "when covered entities discover a cyber incident involving a software product or service provided to such agencies or involving a support system for a software product or service provided to such agencies."	Unknown. Text of proposed rulemaking is not yet public. Policy language: "the time periods within which contractors must report cyber incidents based on a graduated scale of severity, with reporting on the most severe cyber incidents not to exceed 3 days after initial detection."
Notification of customer proprietary network information security breaches	**FCC**	**The Communications Act of 1934** (47 U.S.C. 154, 254(k), 403(b)(2)(B), (c))	Original: **2013** Proposed update: **2022**	**Data breach reporting:** To requires carriers and providers to report data breaches of CPNI.	Private and public disclosure, first to the FBI and the U.S. Secret Service and afterwards to affected customers.	"When a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI."	To the FBI and Secret Service: within seven business days. To the public: after a mandatory waiting period of seven business days with exceptions "in order to avoid immediate and irreparable harm."

Name of Regulation or Other Implementing Framework	Lead Implementing Entity	Key Authorizing Mechanism or Authority; Supplementary Authorities as Applicable	Year Regulation Issued or Effective; Others as Applicable	Scope or Intent of Rule	Private or Public Disclosure	Threshhold for Disclosure	Timeline for Disclosure
Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice	**OCC, Board of the Federal Reserve, the FDIC, and the OTS**	**Gramm-Leach-Bliley Act** (15 U.S.C. 6801) and the **Standards for Safeguarding Customer Information** (15 U.S.C. 6801(b), 6805(b)(2))	Effective: **2005**	**Data breach reporting:** To require financial institutions to report data breaches of non-public information pursuant to the Standards for Safeguarding Customer Information, itself implementing section 501(b) of the Gramm-Leach-Bliley Act, which requires institutions to have a breach response plan.	Public disclosure to affected customers.	Entities must notify affected customers if the institution determines—through an investigation—their information has or reasonably can be misused.	"As soon as possible" if an investigation (by the institution) concludes that information was/could be misused. Includes a delay for law enforcement.
Health Breach Notification Rule	**FTC**	**American Recovery and Reinvestment Act of 2009** (U.S.C. 26 Code note 1) Clarified by: **Statement of the Commission On Breaches by Health Apps and Other Connected Devices**	Effective: **2009** Enforced: **2010**	**Data breach reporting:** To require entities that collect health information but are not covered under HIPAA (including vendors of PHR, PHR-related entities and third party service providers) to report data breaches.	Private and public disclosure. Entities must notify affected individuals. The FTC and state/local media outlets must be notified if the breach affects more than 500 individuals.	Unauthorized acquisition of PHR, which assumes unauthorized use unless proven otherwise by the entity.	Upon discovery of a "breach of security" or up to 60 calendar days. However, if the breach involved more than 500 indivuduals, the FTC must be notified within 10 business days. Both include a delay for law enforcement.
Security Beyond Prevention: The Importance of Effective Breach Disclosures * and Data Breach Response: A Guide for Business (guidance)	**FTC**	**Federal Trade Commission Act** (15 U.S.C. 45) *Note: Guidance based off the rulings of two FTC actions against CafePress and Uber among others, concluding that their failure to notify customers of breach violated Sec. 5 of the FTC Act.	Published: **2022**	**Data breach reporting:** to clarify to FTC-covered entities that the FTC Act has a de facto breach disclosure requirement, since failure to disclose breach can increase likelihood of harm to affected parties (under Section 5 of the FTC Act).	Private and public disclosure. Depending on legal requirements, entities must notify law enforcement, other affected businesses and affected individuals.	Unclear from text of guidance.	Unclear from text of guidance.
Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime	**FinCEN**	**Bank Secrecy Act** (12 U.S.C. 1813 and 1818; 31 U.S.C. 5318 and 5318)	Published: **2016**	**Cyber incident reporting:** To require financial institutions to file suspicious activity reports for cyber events as part of entities' obligations under the BSA.	Private disclosure via a Suspicious Activity Report to FinCEN.	If "cyber-events" or "cyber-enabled crimes" contributed to suspicious transactions involving $5,000 or more as stipulated by the BSA.	No later than 30 calendar days after the activity is detected with a maximum extension of 30 additional days.

Name of Regulation or Other Implementing Framework	Lead Implementing Entity	Key Authorizing Mechanism or Authority; Supplementary Authorities as Applicable	Year Regulation Issued or Effective; Others as Applicable	Scope or Intent of Rule	Private or Public Disclosure	Threshhold for Disclosure	Timeline for Disclosure
Breach Notification Rule, Health Insurance Portability and Accountability Act (HIPAA)	**HHS**	**HIPAA** as updated by the **Health Information Technology for Economic and Clinical Health Act** (42 U.S.C. 17931-34)	Original: **2009** Updated: **2013**	**Data breach reporting:** To require specified healthcare plans, providers or clearinghouses and their associates to notify affected individuals, the HHS and potentially the media of data breaches involving unsecured PHI.	Private and public disclosure. Entities must notify affected individuals, the HHS and—if the breach affects more than 500 individuals—state/local media outlets.	Discovery of a breach compromising unencrypted PHI that poses significant risk according to four factors: 1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; 2) the unauthorized person who used the PHI or to whom the disclosure was made; 3) whether the PHI was actually acquired or viewed; and 4) the extent to which the risk to the PHI has been mitigated.	"Without unreasonable delay" or up to 60 calendar days, with a delay for law enforcement.
CIP-008-6 - Cyber Security Incident Reporting and Response Planning	**NERC**	Ordered updated by FERC via **Order No. 848** (under its authority pursuant to 16 U.S.C. 824o)	Updated: **2019**	**Cyber incident reporting:** To require entities regulated by NERC (specified bulk power/energy systems) to report cybersecurity incidents that compromise or attempt to compromise key specified systems.	Private disclosure to both the relevant Electricity Information Sharing and Analysis Center and, if U.S. based, to CISA Central, formerly US-CERT or the NCCIC.	An incident determined by the entity to have compromised or disrupted one of a pre-specified type of bulk energy system, or its electronic security perimeter or electronic access control or monitoring system.	One hour for "Reportable Cyber Security Incidents." By the end of the next calendar day if an incident attempted to compromise high- or medium-impact systems or identified associated components. New or updated attribution information must be shared within seven calendar days of determination.

Name of Regulation or Other Implementing Framework	Lead Implementing Entity	Key Authorizing Mechanism or Authority; Supplementary Authorities as Applicable	Year Regulation Issued or Effective; Others as Applicable	Scope or Intent of Rule	Private or Public Disclosure	Threshhold for Disclosure	Timeline for Disclosure
Cyber Security Event Notifications	**NRC**	**Atomic Energy Act of 1954** (42 U.S.C. 2073, 2167, 2169, 2201, 2210d, 2210e, 2210h, 2210i, 2273, 2278a, 2282, 2297f); **Energy Reorganization Act of 1974** (42 U.S.C. 5841, 5842); **Nuclear Waste Policy Act of 1982** (42 U.S.C. 10155, 10161; 44 U.S.C. 3504 note)	Effective: **2015** Enforced: **2016**	**Cyber incident reporting:** To clarify the 2009 rule that requires licensees of the NRC to establish a cybersecurity plan by mandating reporting requirements of cyber security incidents to the Commission.	Private disclosure via the NRC's Headquarters Operations Center's Emergency Notification System.	Discovery of an incident impacting safety, security or emergency preparedness functions (including offsite communications) or compromising support systems and equipment that affects these functions.	One hour for events impacting the critical safety functions of systems. Four hours for incidents that may have damaged these same system safety functions.
Title Not Public— "Procedures for reporting known or suspected compromises of [National Security Systems] NSS or otherwise unauthorized access of NSS" (National Security Memorandum 8)	**NSA, with ODNI and CIA**	**Memorandum on improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems** (NSM 8)	Presumed issued: **2022** *Text not public	**Cyber incident reporting:** To require agencies designated as National Security Systems or defense and intelligence systems to report incidents to the NSA and other designated authorities.	Private disclosure to the NSA "through the appropriate Federal Cyber Center or other designated central department point of contact."	Unknown. Per memorandum: any "known or suspected compromise or otherwise unauthorized access" of national security systems or cross-domain solutions that connect to them.	Per the memorandum, either upon agency detection or "upon report by a contractor ... or other federal or non-federal entity."
Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers	**OCC, Board of the Federal Reserve and the FDIC**	Issued within rulemaking authorities under 12 U.S.C. 1, 93a, 161, 481, 1463, 1464, 1861-1867 and 3102 (OCC); 12 U.S.C. 321-338a, 1467a(g), 1818(b), 1844(b), 1861-1867 and 3101 et seq. (Board); 12 U.S.C. 1463, 1811, 1813, 1817, 1819 and 1861-1867 (FDIC)	Issued: **2021** Effective: **2022**	**Cyber incident reporting:** To require banking organizations and banking service providers to report incidents to their relevant federal regulator.	Public and private disclosure to an entity's regulator and to affected customers if disruptions are expected to last four or more hours.	If a "computer-security incident" escalates to a "notfication incident."	No later than 36 hours after determination that an incident has occurred.

Name of Regulation or Other Implementing Framework	Lead Implementing Entity	Key Authorizing Mechanism or Authority; Supplementary Authorities as Applicable	Year Regulation Issued or Effective; Others as Applicable	Scope or Intent of Rule	Private or Public Disclosure	Threshhold for Disclosure	Timeline for Disclosure
Division of Corporation Finance's Disclosure Guidance: Topic No. 2 -- Cybersecurity ("**2011 Guidance**") expanded by the Commission Statement and Guidance on Public Company Cybersecurity Disclosures ("**2018 Guidance**")	**SEC**	Issued within agency rulemaking authority under 15 U.S.C. 77-78	Original: **2011** Update: **2018**	**Cyber incident reporting:** To advise entities regulated by the SEC (public companies) that general securities laws may require them to publicly disclose some cybersecurity risks and incidents to their investors, despite a lack of official cybersecurity disclosure rules.	Public disclosure to current or potential investors via periodic reports.	Discovery of a "material" cybersecurity incident on the company's systems or networks.	Unclear from text of guidance.
Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure	**SEC**	Issued within agency rulemaking authority under 15 U.S.C. 77-78	Draft: **2022**	**Cyber incident reporting:** To require entities regulated by the SEC (public companies) to report material cybersecurity incidents on form 8-K within four days of discovering a material cyber breach.	Public disclosure via Form 8-K.	Discovery of a "material" cybersecurity incident on the company's systems or networks.	Four business days from discovery of materiality.
Security Directive 1580-21-01 (Rail)	**TSA**	Issued within agency rulemaking authority under 49 U.S.C. I 14(l) (2) (A)	Issued: **2021** Expires: Dec. 31, **2022**	**Cyber incident reporting:** To require surface transportation owners and operators (freight railroad carriers identified in 49 CFR 1580.101) to report incidents to CISA.	Private disclosure to CISA.	The discovery of a cybersecurity incident "involving systems that the Owner/Operator has responsibility to operate and/or maintain," as specified on page three of the directive, here.	"... as soon as practicable, but no later than 24 hours after a cybersecurity incident is identified."
Title Not Public— Issued under the **TSA's Aviation Program** (text not public; see reference here)	**TSA**	Issued within agency rulemaking authority over the aviation sector, under 49 U.S.C. I 14(l)(2) (A)	Presumed issued: **2021**	**Cyber incident reporting:** To require designated aviation companies and airports to report cybersecurity incidents to CISA.	Private disclosure to CISA.	Text not public. Threshold is the same as Security Directive Pipeline-2021-01.	Per DHS press release: "as soon as practicable, but no later than 24 hours after a cybersecurity incident is identified." Unable to verify against official text.

Name of Regulation or Other Implementing Framework	Lead Implementing Entity	Key Authorizing Mechanism or Authority; Supplementary Authorities as Applicable	Year Regulation Issued or Effective; Others as Applicable	Scope or Intent of Rule	Private or Public Disclosure	Threshhold for Disclosure	Timeline for Disclosure
Security Directive Pipeline-2021-01	**TSA**	Issued within agency rulemaking authority under 49 U.S.C. I 14(l) (2) (A)	Issued: **2021** Extended as of: May **2022**	**Cyber incident reporting:** To require owners and operators of covered entities in the gas and liquefied national gas sectors (designated "critical" by the TSA) to report specified cybersecurity incidents to CISA.	Private disclosure to CISA.	"... cybersecurity incidents involving systems that the Owner/Operator has responsibility to operate and maintain ..."—as specified on pages 2 and 3 of the directive, here.	"... as soon as practicable, but no later than 12 hours after a cybersecurity incident is identified."

Special Additions

Name of Regulation or Other Implementing Framework	Lead Implementing Entity	Key Authorizing Mechanism or Authority; Supplementary Authorities as Applicable	Year Regulation Issued or Effective; Others as Applicable	Scope or Intent of Rule	Private or Public Disclosure	Threshhold for Disclosure	Timeline for Disclosure
Presidential Policy Directive 41: United States Cyber Incident Coordination	The **NSC** is tasked with coordinating government policy and strategy as needed via the Cyber Response Group (CRG).	Note: PPD 41 is itself a policy document describing intragovernmental coordination efforts that is included in this list for insight into how the executive branch shares major incident information.	Issued: **2016**	**Cyber incident reporting:** To establish lead federal agencies for handling major cyber incidents. Also to require federal cyber incident response agencies to share information with each other. Also to "encourage" private-sector entities experiencing a cyber incident to report the event to law enforcement.	Private; Intragovernmental	N/A	N/A
500.17 Notices to superintendent (pg. 10) *Cited in SEC Commission Statement and Guidance on Public Company Cybersecurity Disclosures ("2018 Guidance")	**NY DFS**	Financial Services Law 102, 201, 202, 301, 302 and 408 Note: This is law in the state of New York.	Promulgated and Effective: **2017**	**Cyber incident reporting:** To require any person operating under or required to operate under a license or similar authorizations under the state's banking, insurance and financial services laws to report cybersecurity incidents to the NY Department of Financial Services (DFS) within 72 hours.	Generally, private disclosure to the Superintendent of the NY DFS, but the SHIELD ACT requires notice to consumers who have been affected by cybersecurity incidents (see FAQ 23).	Cybersecurity incidents that have to be reported to any "government body, self-regulatory agency or any other supervisory body" or ones that can "materially" harm any part of an entitiy's normal operations.	No later than 72 hours.