NRC Draft Cybersecurity Breach Rules -- Required Notifications

Notification	When Required	Duplicate Notifications
One-hour Notification	Within one hour of discovering a cyber attack that "adversely impacted safety-related or important-to-safety function, security functions, or emergency preparedness functions . . . or compromises support systems and equipment that results in adverse impacts to safety, security, or emergency preparedness functions."	
Four-hour Notification	Within four hours of: • Discovering a cyber attack that "could have caused an adverse impact" to safety- and security-related functions; • Discovering a suspected or actual cyber attack that was initiated by personnel with physical or electronic access to computers, communications systems, and networks; and/or • Notification by a local, state, or federal agency of an event related to the implementation of the licensee's cyber security program.	No requirement to make four-hour notification if a one-hour notification is made for the same event.
Eight-hour Notification	Within eight hours of receiving or collecting information about any "observed behavior, activities, or statements" indicating a potential cyber attack.	No requirement to make eight-hour notification if a four-hour notification or one-hour notification is made for the same event.
Twenty-four hour Recordable Events	Licensees should use a corrective action program (as required by 10 C.F.R. § 72.172) to document, track, trend, correct, and prevent recurrence of failures and deficiencies in their cybersecurity program within twenty-four hours of discovery.	A corrective action program should also be used to document, track, and trend one-, four-, and eight-hour notifications.