Table - Freedom of Information Request Reference No: FOI202110031

Incident date:	Licence holder:	Licence site:	Outcome:
9 October 2018	EDF Energy Nuclear Generation Limited (NGL)	Barnwood*	EDF Energy NGL network users received a number of targeted phishing emails from a compromised known third party. EDF Energy NGL blocked access to external web sites hyperlinked within the emails and communications were sent to all recipients of the phishing email asking them to confirm their actions in relation to the phishing email. A further technical review of access to the external web sites was undertaken. All users known to have received the phishing email had their passwords reset as a precaution. There was no indication of compromise to the EDF Energy NGL network. The third-party system falls outside of ONR's regulatory scope.
10-Apr-19	Magnox	Wylfa	New virus scanning tool identified a possible malware virus; remedial action taken.
16-Sep-19	Tradebe (Inutec)	Winfrith	During virus scanning an infected file was discovered on a laptop; remedial action taken.
06-Nov-19	EDF	Hinkley Point B	Malware present on a USB memory stick that was used to download data. The memory stick had no connection to site operating systems and the malware was detected during cyber checks. Infected and potentially infected data quarantined; remedial action taken.
28-Aug-20	National Nuclear Laboratory (NNL)	Preston*	Security tooling identified malware present on a laptop; remedial action taken.
01-Dec-20	Low Level Waste Repository (LLWR)	LLWR	Anomalous data connection identified; remedial action taken.
16-Mar-21	LLWR	LLWR	Anomalous data connection identified; remedial action taken.
09-Aug-21	Magnox	Dungeness A	Anti-viral software scan identified infected file on a PC; remedial action taken.

Notes:
*These are not civil nuclear licensed sites but operate on or in relation to and have been included for completeness.