mittee on Appropriations of the House of Representatives.

(2) CONGRESSIONAL LEADERSHIP.—The term ''congressional leadership'' means—

(A) the majority leader of the Senate;

(B) the minority leader of the Senate;

(C) the Speaker of the House of Representatives; and

(D) the minority leader of the House of Representatives.

(3) SERGEANTS AT ARMS.—The term ''Sergeants at Arms'' means the Sergeant at Arms and Doorkeeper of the Senate, the Sergeant at Arms of the House of Representatives, and the Chief Administrative Officer of the House of Representatives.

DIVISION Y—CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022

SEC. 101. SHORT TITLE.

This division may be cited as the ''Cyber Incident Reporting for Critical Infrastructure Act of 2022''.

SEC. 102. DEFINITIONS.

In this division:

(1) COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT; INFORMATION SYSTEM; RANSOM PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.—The terms ''covered cyber incident'', ''covered entity'', ''cyber incident'', ''information system'', ''ransom payment'', ''ransomware attack'', and ''security vulnerability'' have the meanings given those terms in section 2240 of the Homeland Security Act of 2002, as added by section 103 of this division.

(2) DIRECTOR.—The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency.

SEC. 103. CYBER INCIDENT REPORTING.

(a) CYBER INCIDENT REPORTING.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) in section 2209(c) (6 U.S.C. 659(c))—

(A) in paragraph (11), by striking ''; and'' and inserting a semicolon;

(B) in paragraph (12), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(13) receiving, aggregating, and analyzing reports related to covered cyber incidents (as defined

in section 2240) submitted by covered entities (as defined in section 2240) and reports related to ransom payments (as defined in section 2240) submitted by covered entities (as defined in section 2240) in furtherance of the activities specified in sections 2202(e), 2203, and 2241, this subsection, and any other authorized activity of the Director, to enhance the situational awareness of cybersecurity threats across critical infrastructure sectors.''; and

(2) by adding at the end the following:

"Subtitle D—Cyber Incident Reporting

"SEC. 2240. DEFINITIONS.

''In this subtitle:

''(1) CENTER.—The term 'Center' means the center established under section 2209.

''(2) CLOUD SERVICE PROVIDER.—The term 'cloud service provider' means an entity offering products or services related to cloud computing, as defined by the National Institute of Standards and Technology in NIST Special Publication 800–145 and any amendatory or superseding document relating thereto.

''(3) COUNCIL.—The term 'Council' means the Cyber Incident Reporting Council described in section 2246.

''(4) COVERED CYBER INCIDENT.—The term 'covered cyber incident' means a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the final rule issued pursuant to section 2242(b).

''(5) COVERED ENTITY.—The term 'covered entity' means an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director in the final rule issued pursuant to section 2242(b).

''(6) CYBER INCIDENT.—The term 'cyber incident'—

''(A) has the meaning given the term 'incident' in section 2209; and

''(B) does not include an occurrence that imminently, but not actually, jeopardizes—

''(i) information on information systems; or

''(ii) information systems.

''(7) CYBER THREAT.—The term 'cyber threat' has the meaning given the term 'cybersecurity threat' in section 2201.

''(8) CYBER THREAT INDICATOR; CYBERSECURITY PURPOSE; DEFENSIVE MEASURE; FEDERAL ENTITY; SECURITY VULNERABILITY.—The terms 'cyber threat indicator', 'cybersecurity purpose', 'defensive measure', 'Federal entity', and 'security vulnerability' have the meanings given those terms in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

''(9) INCIDENT; SHARING.—The terms 'incident' and 'sharing' have the meanings given those terms in section 2209.

''(10) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term 'Information Sharing and Analysis Organization' has the meaning given the term in section 2222.

''(11) INFORMATION SYSTEM.—The term 'information system'—

''(A) has the meaning given the term in section 3502 of title 44, United States Code; and

''(B) includes industrial control systems, such as supervisory control and data acquisition

systems, distributed control systems, and programmable logic controllers.

''(12) MANAGED SERVICE PROVIDER.—The term 'managed service provider' means an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity (such as hosting), or in a third party data center.

''(13) RANSOM PAYMENT.—The term 'ransom payment' means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack.

''(14) RANSOMWARE ATTACK.—The term 'ransomware attack'—

''(A) means an incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, avail-

ability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and

"(B) does not include any such event where the demand for payment is—

"(i) not genuine; or

"(ii) made in good faith by an entity in response to a specific request by the owner or operator of the information system.

"(15) SECTOR RISK MANAGEMENT AGENCY.—The term 'Sector Risk Management Agency' has the meaning given the term in section 2201.

"(16) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cyber incident, or a group of related cyber incidents, that the Secretary determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States.

"(17) SUPPLY CHAIN COMPROMISE.—The term 'supply chain compromise' means an incident within the supply chain of an information system that an

adversary can leverage or does leverage to jeopardize the confidentiality, integrity, or availability of the information system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle.

''(18) VIRTUAL CURRENCY.—The term 'virtual currency' means the digital representation of value that functions as a medium of exchange, a unit of account, or a store of value.

''(19) VIRTUAL CURRENCY ADDRESS.—The term 'virtual currency address' means a unique public cryptographic key identifying the location to which a virtual currency payment can be made.

''SEC. 2241. CYBER INCIDENT REVIEW.

''(a) ACTIVITIES.—The Center shall—

''(1) receive, aggregate, analyze, and secure, using processes consistent with the processes developed pursuant to the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.) reports from covered entities related to a covered cyber incident to assess the effectiveness of security controls, identify tactics, techniques, and procedures adversaries use to overcome those controls and other cybersecurity purposes, including to assess potential impact of cyber incidents on public health and safety

and to enhance situational awareness of cyber threats across critical infrastructure sectors;

''(2) coordinate and share information with appropriate Federal departments and agencies to identify and track ransom payments, including those utilizing virtual currencies;

''(3) leverage information gathered about cyber incidents to—

''(A) enhance the quality and effectiveness of information sharing and coordination efforts with appropriate entities, including agencies, sector coordinating councils, Information Sharing and Analysis Organizations, State, local, Tribal, and territorial governments, technology providers, critical infrastructure owners and operators, cybersecurity and cyber incident response firms, and security researchers; and

''(B) provide appropriate entities, including sector coordinating councils, Information Sharing and Analysis Organizations, State, local, Tribal, and territorial governments, technology providers, cybersecurity and cyber incident response firms, and security researchers, with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including,

to the maximum extent practicable, related contextual information, cyber threat indicators, and defensive measures, pursuant to section 2245;

''(4) establish mechanisms to receive feedback from stakeholders on how the Agency can most effectively receive covered cyber incident reports, ransom payment reports, and other voluntarily provided information, and how the Agency can most effectively support private sector cybersecurity;

''(5) facilitate the timely sharing, on a voluntary basis, between relevant critical infrastructure owners and operators of information relating to covered cyber incidents and ransom payments, particularly with respect to ongoing cyber threats or security vulnerabilities and identify and disseminate ways to prevent or mitigate similar cyber incidents in the future;

''(6) for a covered cyber incident, including a ransomware attack, that also satisfies the definition of a significant cyber incident, or is part of a group of related cyber incidents that together satisfy such definition, conduct a review of the details surrounding the covered cyber incident or group of those incidents and identify and disseminate ways to prevent or mitigate similar incidents in the future;

''(7) with respect to covered cyber incident reports under section 2242(a) and 2243 involving an ongoing cyber threat or security vulnerability, immediately review those reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders, in coordination with other divisions within the Agency, as appropriate;

''(8) publish quarterly unclassified, public reports that describe aggregated, anonymized observations, findings, and recommendations based on covered cyber incident reports, which may be based on the unclassified information contained in the briefings required under subsection (c);

''(9) proactively identify opportunities, consistent with the protections in section 2245, to leverage and utilize data on cyber incidents in a manner that enables and strengthens cybersecurity research carried out by academic institutions and other private sector organizations, to the greatest extent practicable; and

''(10) in accordance with section 2245 and subsection (b) of this section, as soon as possible but not later than 24 hours after receiving a covered cyber incident report, ransom payment report, volun-

tarily submitted information pursuant to section 2243, or information received pursuant to a request for information or subpoena under section 2244, make available the information to appropriate Sector Risk Management Agencies and other appropriate Federal agencies.

''(b) INTERAGENCY SHARING.—The President or a designee of the President—

''(1) may establish a specific time requirement for sharing information under subsection (a)(10); and

''(2) shall determine the appropriate Federal agencies under subsection (a)(10).

''(c) PERIODIC BRIEFING.—Not later than 60 days after the effective date of the final rule required under section 2242(b), and on the first day of each month thereafter, the Director, in consultation with the National Cyber Director, the Attorney General, and the Director of National Intelligence, shall provide to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a briefing that characterizes the

national cyber threat landscape, including the threat facing Federal agencies and covered entities, and applicable intelligence and law enforcement information, covered cyber incidents, and ransomware attacks, as of the date of the briefing, which shall—

''(1) include the total number of reports submitted under sections 2242 and 2243 during the preceding month, including a breakdown of required and voluntary reports;

''(2) include any identified trends in covered cyber incidents and ransomware attacks over the course of the preceding month and as compared to previous reports, including any trends related to the information collected in the reports submitted under sections 2242 and 2243, including—

''(A) the infrastructure, tactics, and techniques malicious cyber actors commonly use; and

''(B) intelligence gaps that have impeded, or currently are impeding, the ability to counter covered cyber incidents and ransomware threats;

''(3) include a summary of the known uses of the information in reports submitted under sections 2242 and 2243; and

''(4) include an unclassified portion, but may include a classified component.

''SEC. 2242. REQUIRED REPORTING OF CERTAIN CYBER INCIDENTS.

''(a) IN GENERAL.—

''(1) COVERED CYBER INCIDENT REPORTS.—

''(A) IN GENERAL.—A covered entity that experiences a covered cyber incident shall report the covered cyber incident to the Agency not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.

''(B) LIMITATION.—The Director may not require reporting under subparagraph (A) any earlier than 72 hours after the covered entity reasonably believes that a covered cyber incident has occurred.

''(2) RANSOM PAYMENT REPORTS.—

''(A) IN GENERAL.—A covered entity that makes a ransom payment as the result of a ransomware attack against the covered entity shall report the payment to the Agency not later than 24 hours after the ransom payment has been made.

''(B) APPLICATION.—The requirements under subparagraph (A) shall apply even if the ransomware attack is not a covered cyber incident subject to the reporting requirements under paragraph (1).

''(3) SUPPLEMENTAL REPORTS.—A covered entity shall promptly submit to the Agency an update or supplement to a previously submitted covered cyber incident report if substantial new or different information becomes available or if the covered entity makes a ransom payment after submitting a covered cyber incident report required under paragraph (1), until such date that such covered entity notifies the Agency that the covered cyber incident at issue has concluded and has been fully mitigated and resolved.

''(4) PRESERVATION OF INFORMATION.—Any covered entity subject to requirements of paragraph (1), (2), or (3) shall preserve data relevant to the covered cyber incident or ransom payment in accordance with procedures established in the final rule issued pursuant to subsection (b).

''(5) EXCEPTIONS.—

''(A) REPORTING OF COVERED CYBER INCIDENT WITH RANSOM PAYMENT.—If a covered

entity is the victim of a covered cyber incident and makes a ransom payment prior to the 72 hour requirement under paragraph (1), such that the reporting requirements under paragraphs (1) and (2) both apply, the covered entity may submit a single report to satisfy the requirements of both paragraphs in accordance with procedures established in the final rule issued pursuant to subsection (b).

''(B) SUBSTANTIALLY SIMILAR REPORTED INFORMATION.—

''(i) IN GENERAL.—Subject to the limitation described in clause (ii), where the Agency has an agreement in place that satisfies the requirements of section 104(a) of the Cyber Incident Reporting for Critical Infrastructure Act of 2022, the requirements under paragraphs (1), (2), and (3) shall not apply to a covered entity required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe.

''(ii) LIMITATION.—The exemption in clause (i) shall take effect with respect to

mittee on Appropriations of the House of Representatives.

(2) CONGRESSIONAL LEADERSHIP.—The term ''congressional leadership'' means—

(A) the majority leader of the Senate;

(B) the minority leader of the Senate;

(C) the Speaker of the House of Representatives; and

(D) the minority leader of the House of Representatives.

(3) SERGEANTS AT ARMS.—The term ''Sergeants at Arms'' means the Sergeant at Arms and Doorkeeper of the Senate, the Sergeant at Arms of the House of Representatives, and the Chief Administrative Officer of the House of Representatives.

DIVISION Y—CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022

SEC. 101. SHORT TITLE.

This division may be cited as the ''Cyber Incident Reporting for Critical Infrastructure Act of 2022''.

SEC. 102. DEFINITIONS.

In this division:

(1) COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT; INFORMATION SYSTEM; RANSOM PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.—The terms ''covered cyber incident'', ''covered entity'', ''cyber incident'', ''information system'', ''ransom payment'', ''ransomware attack'', and ''security vulnerability'' have the meanings given those terms in section 2240 of the Homeland Security Act of 2002, as added by section 103 of this division.

(2) DIRECTOR.—The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency.

SEC. 103. CYBER INCIDENT REPORTING.

(a) CYBER INCIDENT REPORTING.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) in section 2209(c) (6 U.S.C. 659(c))—

(A) in paragraph (11), by striking ''; and'' and inserting a semicolon;

(B) in paragraph (12), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(13) receiving, aggregating, and analyzing reports related to covered cyber incidents (as defined

in section 2240) submitted by covered entities (as defined in section 2240) and reports related to ransom payments (as defined in section 2240) submitted by covered entities (as defined in section 2240) in furtherance of the activities specified in sections 2202(e), 2203, and 2241, this subsection, and any other authorized activity of the Director, to enhance the situational awareness of cybersecurity threats across critical infrastructure sectors.''; and

(2) by adding at the end the following:

"Subtitle D—Cyber Incident Reporting

"SEC. 2240. DEFINITIONS.

''In this subtitle:

''(1) CENTER.—The term 'Center' means the center established under section 2209.

''(2) CLOUD SERVICE PROVIDER.—The term 'cloud service provider' means an entity offering products or services related to cloud computing, as defined by the National Institute of Standards and Technology in NIST Special Publication 800–145 and any amendatory or superseding document relating thereto.

''(3) COUNCIL.—The term 'Council' means the Cyber Incident Reporting Council described in section 2246.

''(4) COVERED CYBER INCIDENT.—The term 'covered cyber incident' means a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the final rule issued pursuant to section 2242(b).

''(5) COVERED ENTITY.—The term 'covered entity' means an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director in the final rule issued pursuant to section 2242(b).

''(6) CYBER INCIDENT.—The term 'cyber incident'—

''(A) has the meaning given the term 'incident' in section 2209; and

''(B) does not include an occurrence that imminently, but not actually, jeopardizes—

''(i) information on information systems; or

''(ii) information systems.

''(7) CYBER THREAT.—The term 'cyber threat' has the meaning given the term 'cybersecurity threat' in section 2201.

''(8) CYBER THREAT INDICATOR; CYBERSECURITY PURPOSE; DEFENSIVE MEASURE; FEDERAL ENTITY; SECURITY VULNERABILITY.—The terms 'cyber threat indicator', 'cybersecurity purpose', 'defensive measure', 'Federal entity', and 'security vulnerability' have the meanings given those terms in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

''(9) INCIDENT; SHARING.—The terms 'incident' and 'sharing' have the meanings given those terms in section 2209.

''(10) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term 'Information Sharing and Analysis Organization' has the meaning given the term in section 2222.

''(11) INFORMATION SYSTEM.—The term 'information system'—

''(A) has the meaning given the term in section 3502 of title 44, United States Code; and

''(B) includes industrial control systems, such as supervisory control and data acquisition

systems, distributed control systems, and programmable logic controllers.

''(12) MANAGED SERVICE PROVIDER.—The term 'managed service provider' means an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity (such as hosting), or in a third party data center.

''(13) RANSOM PAYMENT.—The term 'ransom payment' means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack.

''(14) RANSOMWARE ATTACK.—The term 'ransomware attack'—

''(A) means an incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, avail-

ability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and

"(B) does not include any such event where the demand for payment is—

"(i) not genuine; or

"(ii) made in good faith by an entity in response to a specific request by the owner or operator of the information system.

"(15) SECTOR RISK MANAGEMENT AGENCY.—The term 'Sector Risk Management Agency' has the meaning given the term in section 2201.

"(16) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cyber incident, or a group of related cyber incidents, that the Secretary determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States.

"(17) SUPPLY CHAIN COMPROMISE.—The term 'supply chain compromise' means an incident within the supply chain of an information system that an

adversary can leverage or does leverage to jeopardize the confidentiality, integrity, or availability of the information system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle.

''(18) VIRTUAL CURRENCY.—The term 'virtual currency' means the digital representation of value that functions as a medium of exchange, a unit of account, or a store of value.

''(19) VIRTUAL CURRENCY ADDRESS.—The term 'virtual currency address' means a unique public cryptographic key identifying the location to which a virtual currency payment can be made.

''SEC. 2241. CYBER INCIDENT REVIEW.

''(a) ACTIVITIES.—The Center shall—

''(1) receive, aggregate, analyze, and secure, using processes consistent with the processes developed pursuant to the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.) reports from covered entities related to a covered cyber incident to assess the effectiveness of security controls, identify tactics, techniques, and procedures adversaries use to overcome those controls and other cybersecurity purposes, including to assess potential impact of cyber incidents on public health and safety

and to enhance situational awareness of cyber threats across critical infrastructure sectors;

''(2) coordinate and share information with appropriate Federal departments and agencies to identify and track ransom payments, including those utilizing virtual currencies;

''(3) leverage information gathered about cyber incidents to—

''(A) enhance the quality and effectiveness of information sharing and coordination efforts with appropriate entities, including agencies, sector coordinating councils, Information Sharing and Analysis Organizations, State, local, Tribal, and territorial governments, technology providers, critical infrastructure owners and operators, cybersecurity and cyber incident response firms, and security researchers; and

''(B) provide appropriate entities, including sector coordinating councils, Information Sharing and Analysis Organizations, State, local, Tribal, and territorial governments, technology providers, cybersecurity and cyber incident response firms, and security researchers, with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including,

to the maximum extent practicable, related contextual information, cyber threat indicators, and defensive measures, pursuant to section 2245;

''(4) establish mechanisms to receive feedback from stakeholders on how the Agency can most effectively receive covered cyber incident reports, ransom payment reports, and other voluntarily provided information, and how the Agency can most effectively support private sector cybersecurity;

''(5) facilitate the timely sharing, on a voluntary basis, between relevant critical infrastructure owners and operators of information relating to covered cyber incidents and ransom payments, particularly with respect to ongoing cyber threats or security vulnerabilities and identify and disseminate ways to prevent or mitigate similar cyber incidents in the future;

''(6) for a covered cyber incident, including a ransomware attack, that also satisfies the definition of a significant cyber incident, or is part of a group of related cyber incidents that together satisfy such definition, conduct a review of the details surrounding the covered cyber incident or group of those incidents and identify and disseminate ways to prevent or mitigate similar incidents in the future;

''(7) with respect to covered cyber incident reports under section 2242(a) and 2243 involving an ongoing cyber threat or security vulnerability, immediately review those reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders, in coordination with other divisions within the Agency, as appropriate;

''(8) publish quarterly unclassified, public reports that describe aggregated, anonymized observations, findings, and recommendations based on covered cyber incident reports, which may be based on the unclassified information contained in the briefings required under subsection (c);

''(9) proactively identify opportunities, consistent with the protections in section 2245, to leverage and utilize data on cyber incidents in a manner that enables and strengthens cybersecurity research carried out by academic institutions and other private sector organizations, to the greatest extent practicable; and

''(10) in accordance with section 2245 and subsection (b) of this section, as soon as possible but not later than 24 hours after receiving a covered cyber incident report, ransom payment report, volun-

tarily submitted information pursuant to section 2243, or information received pursuant to a request for information or subpoena under section 2244, make available the information to appropriate Sector Risk Management Agencies and other appropriate Federal agencies.

''(b) INTERAGENCY SHARING.—The President or a designee of the President—

''(1) may establish a specific time requirement for sharing information under subsection (a)(10); and

''(2) shall determine the appropriate Federal agencies under subsection (a)(10).

''(c) PERIODIC BRIEFING.—Not later than 60 days after the effective date of the final rule required under section 2242(b), and on the first day of each month thereafter, the Director, in consultation with the National Cyber Director, the Attorney General, and the Director of National Intelligence, shall provide to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a briefing that characterizes the

national cyber threat landscape, including the threat facing Federal agencies and covered entities, and applicable intelligence and law enforcement information, covered cyber incidents, and ransomware attacks, as of the date of the briefing, which shall—

''(1) include the total number of reports submitted under sections 2242 and 2243 during the preceding month, including a breakdown of required and voluntary reports;

''(2) include any identified trends in covered cyber incidents and ransomware attacks over the course of the preceding month and as compared to previous reports, including any trends related to the information collected in the reports submitted under sections 2242 and 2243, including—

''(A) the infrastructure, tactics, and techniques malicious cyber actors commonly use; and

''(B) intelligence gaps that have impeded, or currently are impeding, the ability to counter covered cyber incidents and ransomware threats;

''(3) include a summary of the known uses of the information in reports submitted under sections 2242 and 2243; and

''(4) include an unclassified portion, but may include a classified component.

''SEC. 2242. REQUIRED REPORTING OF CERTAIN CYBER INCIDENTS.

''(a) IN GENERAL.—

''(1) COVERED CYBER INCIDENT REPORTS.—

''(A) IN GENERAL.—A covered entity that experiences a covered cyber incident shall report the covered cyber incident to the Agency not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.

''(B) LIMITATION.—The Director may not require reporting under subparagraph (A) any earlier than 72 hours after the covered entity reasonably believes that a covered cyber incident has occurred.

''(2) RANSOM PAYMENT REPORTS.—

''(A) IN GENERAL.—A covered entity that makes a ransom payment as the result of a ransomware attack against the covered entity shall report the payment to the Agency not later than 24 hours after the ransom payment has been made.

''(B) APPLICATION.—The requirements under subparagraph (A) shall apply even if the ransomware attack is not a covered cyber incident subject to the reporting requirements under paragraph (1).

''(3) SUPPLEMENTAL REPORTS.—A covered entity shall promptly submit to the Agency an update or supplement to a previously submitted covered cyber incident report if substantial new or different information becomes available or if the covered entity makes a ransom payment after submitting a covered cyber incident report required under paragraph (1), until such date that such covered entity notifies the Agency that the covered cyber incident at issue has concluded and has been fully mitigated and resolved.

''(4) PRESERVATION OF INFORMATION.—Any covered entity subject to requirements of paragraph (1), (2), or (3) shall preserve data relevant to the covered cyber incident or ransom payment in accordance with procedures established in the final rule issued pursuant to subsection (b).

''(5) EXCEPTIONS.—

''(A) REPORTING OF COVERED CYBER INCIDENT WITH RANSOM PAYMENT.—If a covered

entity is the victim of a covered cyber incident and makes a ransom payment prior to the 72 hour requirement under paragraph (1), such that the reporting requirements under paragraphs (1) and (2) both apply, the covered entity may submit a single report to satisfy the requirements of both paragraphs in accordance with procedures established in the final rule issued pursuant to subsection (b).

''(B) SUBSTANTIALLY SIMILAR REPORTED INFORMATION.—

''(i) IN GENERAL.—Subject to the limitation described in clause (ii), where the Agency has an agreement in place that satisfies the requirements of section 104(a) of the Cyber Incident Reporting for Critical Infrastructure Act of 2022, the requirements under paragraphs (1), (2), and (3) shall not apply to a covered entity required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe.

''(ii) LIMITATION.—The exemption in clause (i) shall take effect with respect to

a covered entity once an agency agreement and sharing mechanism is in place between the Agency and the respective Federal agency, pursuant to section 104(a) of the Cyber Incident Reporting for Critical Infrastructure Act of 2022.

''(iii) RULES OF CONSTRUCTION.—Nothing in this paragraph shall be construed to—

''(I) exempt a covered entity from the reporting requirements under paragraph (3) unless the supplemental report also meets the requirements of clauses (i) and (ii) of this paragraph;

''(II) prevent the Agency from contacting an entity submitting information to another Federal agency that is provided to the Agency pursuant to section 104 of the Cyber Incident Reporting for Critical Infrastructure Act of 2022; or

''(III) prevent an entity from communicating with the Agency.

''(C) DOMAIN NAME SYSTEM.—The requirements under paragraphs (1), (2) and (3) shall not apply to a covered entity or the functions of a covered entity that the Director determines constitute critical infrastructure owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the Domain Name System, such as the Internet Corporation for Assigned Names and Numbers or the Internet Assigned Numbers Authority.

''(6) MANNER, TIMING, AND FORM OF REPORTS.—Reports made under paragraphs (1), (2), and (3) shall be made in the manner and form, and within the time period in the case of reports made under paragraph (3), prescribed in the final rule issued pursuant to subsection (b).

''(7) EFFECTIVE DATE.—Paragraphs (1) through (4) shall take effect on the dates prescribed in the final rule issued pursuant to subsection (b).

''(b) RULEMAKING.—

''(1) NOTICE OF PROPOSED RULEMAKING.—Not later than 24 months after the date of enactment of this section, the Director, in consultation with Sector Risk Management Agencies, the Department of Jus-

tice, and other Federal agencies, shall publish in the Federal Register a notice of proposed rulemaking to implement subsection (a).

''(2) FINAL RULE.—Not later than 18 months after publication of the notice of proposed rulemaking under paragraph (1), the Director shall issue a final rule to implement subsection (a).

''(3) SUBSEQUENT RULEMAKINGS.—

''(A) IN GENERAL.—The Director is authorized to issue regulations to amend or revise the final rule issued pursuant to paragraph (2).

''(B) PROCEDURES.—Any subsequent rules issued under subparagraph (A) shall comply with the requirements under chapter 5 of title 5, United States Code, including the issuance of a notice of proposed rulemaking under section 553 of such title.

''(c) ELEMENTS.—The final rule issued pursuant to subsection (b) shall be composed of the following elements:

''(1) A clear description of the types of entities that constitute covered entities, based on—

''(A) the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety;

''(B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and

''(C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure.

''(2) A clear description of the types of substantial cyber incidents that constitute covered cyber incidents, which shall—

''(A) at a minimum, require the occurrence of—

''(i) a cyber incident that leads to substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes;

''(ii) a disruption of business or industrial operations, including due to a denial of service attack, ransomware attack, or

exploitation of a zero day vulnerability, against

''(I) an information system or network; or

''(II) an operational technology system or process; or

''(iii) unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise;

''(B) consider—

''(i) the sophistication or novelty of the tactics used to perpetrate such a cyber incident, as well as the type, volume, and sensitivity of the data at issue;

''(ii) the number of individuals directly or indirectly affected or potentially affected by such a cyber incident; and

''(iii) potential impacts on industrial control systems, such as supervisory control and data acquisition systems, distrib-

uted control systems, and programmable logic controllers; and

''(C) exclude—

''(i) any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system; and

''(ii) the threat of disruption as extortion, as described in section 2240(14)(A).

''(3) A requirement that, if a covered cyber incident or a ransom payment occurs following an exempted threat described in paragraph (2)(C)(ii), the covered entity shall comply with the requirements in this subtitle in reporting the covered cyber incident or ransom payment.

''(4) A clear description of the specific required contents of a report pursuant to subsection (a)(1), which shall include the following information, to the extent applicable and available, with respect to a covered cyber incident:

''(A) A description of the covered cyber incident, including—

''(i) identification and a description of the function of the affected information

systems, networks, or devices that were, or are reasonably believed to have been, affected by such cyber incident;

''(ii) a description of the unauthorized access with substantial loss of confidentiality, integrity, or availability of the affected information system or network or disruption of business or industrial operations;

''(iii) the estimated date range of such incident; and

''(iv) the impact to the operations of the covered entity.

''(B) Where applicable, a description of the vulnerabilities exploited and the security defenses that were in place, as well as the tactics, techniques, and procedures used to perpetrate the covered cyber incident.

''(C) Where applicable, any identifying or contact information related to each actor reasonably believed to be responsible for such cyber incident.

''(D) Where applicable, identification of the category or categories of information that were, or are reasonably believed to have been,

accessed or acquired by an unauthorized person.

''(E) The name and other information that clearly identifies the covered entity impacted by the covered cyber incident, including, as applicable, the State of incorporation or formation of the covered entity, trade names, legal names, or other identifiers.

''(F) Contact information, such as telephone number or electronic mail address, that the Agency may use to contact the covered entity or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission of, and at the direction of, the covered entity to assist with compliance with the requirements of this subtitle.

''(5) A clear description of the specific required contents of a report pursuant to subsection (a)(2), which shall be the following information, to the extent applicable and available, with respect to a ransom payment:

''(A) A description of the ransomware attack, including the estimated date range of the attack.

''(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetrate the ransomware attack.

''(C) Where applicable, any identifying or contact information related to the actor or actors reasonably believed to be responsible for the ransomware attack.

''(D) The name and other information that clearly identifies the covered entity that made the ransom payment or on whose behalf the payment was made.

''(E) Contact information, such as telephone number or electronic mail address, that the Agency may use to contact the covered entity that made the ransom payment or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission of, and at the direction of, that covered entity to assist with compliance with the requirements of this subtitle.

''(F) The date of the ransom payment.

"(G) The ransom payment demand, including the type of virtual currency or other commodity requested, if applicable.

"(H) The ransom payment instructions, including information regarding where to send the payment, such as the virtual currency address or physical address the funds were requested to be sent to, if applicable.

"(I) The amount of the ransom payment.

"(6) A clear description of the types of data required to be preserved pursuant to subsection (a)(4), the period of time for which the data is required to be preserved, and allowable uses, processes, and procedures.

"(7) Deadlines and criteria for submitting supplemental reports to the Agency required under subsection (a)(3), which shall—

"(A) be established by the Director in consultation with the Council;

"(B) consider any existing regulatory reporting requirements similar in scope, purpose, and timing to the reporting requirements to which such a covered entity may also be subject, and make efforts to harmonize the timing

and contents of any such reports to the maximum extent practicable;

''(C) balance the need for situational awareness with the ability of the covered entity to conduct cyber incident response and investigations; and

''(D) provide a clear description of what constitutes substantial new or different information.

''(8) Procedures for—

''(A) entities, including third parties pursuant to subsection (d)(1), to submit reports required by paragraphs (1), (2), and (3) of subsection (a), including the manner and form thereof, which shall include, at a minimum, a concise, user-friendly web-based form;

''(B) the Agency to carry out—

''(i) the enforcement provisions of section 2244, including with respect to the issuance, service, withdrawal, referral process, and enforcement of subpoenas, appeals and due process procedures;

''(ii) other available enforcement mechanisms including acquisition, suspension and debarment procedures; and

"(iii) other aspects of noncompliance;

"(C) implementing the exceptions provided in subsection (a)(5); and

"(D) protecting privacy and civil liberties consistent with processes adopted pursuant to section 105(b) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(b)) and anonymizing and safeguarding, or no longer retaining, information received and disclosed through covered cyber incident reports and ransom payment reports that is known to be personal information of a specific individual or information that identifies a specific individual that is not directly related to a cybersecurity threat.

"(9) Other procedural measures directly necessary to implement subsection (a).

"(d) THIRD PARTY REPORT SUBMISSION AND RANSOM PAYMENT.—

"(1) REPORT SUBMISSION.—A covered entity that is required to submit a covered cyber incident report or a ransom payment report may use a third party, such as an incident response company, insurance provider, service provider, Information Sharing and Analysis Organization, or law firm, to submit the required report under subsection (a).

''(2) RANSOM PAYMENT.—If a covered entity impacted by a ransomware attack uses a third party to make a ransom payment, the third party shall not be required to submit a ransom payment report for itself under subsection (a)(2).

''(3) DUTY TO REPORT.—Third-party reporting under this subparagraph does not relieve a covered entity from the duty to comply with the requirements for covered cyber incident report or ransom payment report submission.

''(4) RESPONSIBILITY TO ADVISE.—Any third party used by a covered entity that knowingly makes a ransom payment on behalf of a covered entity impacted by a ransomware attack shall advise the impacted covered entity of the responsibilities of the impacted covered entity regarding reporting ransom payments under this section.

''(e) OUTREACH TO COVERED ENTITIES.—

''(1) IN GENERAL.—The Agency shall conduct an outreach and education campaign to inform likely covered entities, entities that offer or advertise as a service to customers to make or facilitate ransom payments on behalf of covered entities impacted by ransomware attacks and other appropriate entities

of the requirements of paragraphs (1), (2), and (3) of subsection (a).

''(2) ELEMENTS.—The outreach and education campaign under paragraph (1) shall include the following:

''(A) An overview of the final rule issued pursuant to subsection (b).

''(B) An overview of mechanisms to submit to the Agency covered cyber incident reports, ransom payment reports, and information relating to the disclosure, retention, and use of covered cyber incident reports and ransom payment reports under this section.

''(C) An overview of the protections afforded to covered entities for complying with the requirements under paragraphs (1), (2), and (3) of subsection (a).

''(D) An overview of the steps taken under section 2244 when a covered entity is not in compliance with the reporting requirements under subsection (a).

''(E) Specific outreach to cybersecurity vendors, cyber incident response providers, cybersecurity insurance entities, and other entities that may support covered entities.

"(F) An overview of the privacy and civil liberties requirements in this subtitle.

"(3) COORDINATION.—In conducting the outreach and education campaign required under paragraph (1), the Agency may coordinate with—

"(A) the Critical Infrastructure Partnership Advisory Council established under section 871;

"(B) Information Sharing and Analysis Organizations;

"(C) trade associations;

"(D) information sharing and analysis centers;

"(E) sector coordinating councils; and

"(F) any other entity as determined appropriate by the Director.

"(f) EXEMPTION.—Sections 3506(c), 3507, 3508, and 3509 of title 44, United States Code, shall not apply to any action to carry out this section.

"(g) RULE OF CONSTRUCTION.—Nothing in this section shall affect the authorities of the Federal Government to implement the requirements of Executive Order 14028 (86 Fed. Reg. 26633; relating to improving the nation's cybersecurity), including changes to the Federal Acquisi-

tion Regulations and remedies to include suspension and debarment.

''(h) SAVINGS PROVISION.—Nothing in this section shall be construed to supersede or to abrogate, modify, or otherwise limit the authority that is vested in any officer or any agency of the United States Government to regulate or take action with respect to the cybersecurity of an entity.

''SEC. 2243. VOLUNTARY REPORTING OF OTHER CYBER INCIDENTS.

''(a) IN GENERAL.—Entities may voluntarily report cyber incidents or ransom payments to the Agency that are not required under paragraph (1), (2), or (3) of section 2242(a), but may enhance the situational awareness of cyber threats.

''(b) VOLUNTARY PROVISION OF ADDITIONAL INFORMATION IN REQUIRED REPORTS.—Covered entities may voluntarily include in reports required under paragraph (1), (2), or (3) of section 2242(a) information that is not required to be included, but may enhance the situational awareness of cyber threats.

''(c) APPLICATION OF PROTECTIONS.—The protections under section 2245 applicable to reports made under section 2242 shall apply in the same manner and to the

same extent to reports and information submitted under subsections (a) and (b).

"SEC. 2244. NONCOMPLIANCE WITH REQUIRED REPORTING.

"(a) PURPOSE.—In the event that a covered entity that is required to submit a report under section 2242(a) fails to comply with the requirement to report, the Director may obtain information about the cyber incident or ransom payment by engaging the covered entity directly to request information about the cyber incident or ransom payment, and if the Director is unable to obtain information through such engagement, by issuing a subpoena to the covered entity, pursuant to subsection (c), to gather information sufficient to determine whether a covered cyber incident or ransom payment has occurred.

"(b) INITIAL REQUEST FOR INFORMATION.—

"(1) IN GENERAL.—If the Director has reason to believe, whether through public reporting or other information in the possession of the Federal Government, including through analysis performed pursuant to paragraph (1) or (2) of section 2241(a), that a covered entity has experienced a covered cyber incident or made a ransom payment but failed to report such cyber incident or payment to the Agency in accordance with section 2242(a), the Director may request additional information from the covered

entity to confirm whether or not a covered cyber incident or ransom payment has occurred.

''(2) TREATMENT.—Information provided to the Agency in response to a request under paragraph (1) shall be treated as if it was submitted through the reporting procedures established in section 2242.

''(c) ENFORCEMENT.—

''(1) IN GENERAL.—If, after the date that is 72 hours from the date on which the Director made the request for information in subsection (b), the Director has received no response from the covered entity from which such information was requested, or received an inadequate response, the Director may issue to such covered entity a subpoena to compel disclosure of information the Director deems necessary to determine whether a covered cyber incident or ransom payment has occurred and obtain the information required to be reported pursuant to section 2242 and any implementing regulations, and assess potential impacts to national security, economic security, or public health and safety.

''(2) CIVIL ACTION.—

''(A) IN GENERAL.—If a covered entity fails to comply with a subpoena, the Director may refer the matter to the Attorney General

to bring a civil action in a district court of the United States to enforce such subpoena.

''(B) VENUE.—An action under this paragraph may be brought in the judicial district in which the covered entity against which the action is brought resides, is found, or does business.

''(C) CONTEMPT OF COURT.—A court may punish a failure to comply with a subpoena issued under this subsection as contempt of court.

''(3) NON-DELEGATION.—The authority of the Director to issue a subpoena under this subsection may not be delegated.

''(4) AUTHENTICATION.—

''(A) IN GENERAL.—Any subpoena issued electronically pursuant to this subsection shall be authenticated with a cryptographic digital signature of an authorized representative of the Agency, or other comparable successor technology, that allows the Agency to demonstrate that such subpoena was issued by the Agency and has not been altered or modified since such issuance.

"(B) INVALID IF NOT AUTHENTICATED.—Any subpoena issued electronically pursuant to this subsection that is not authenticated in accordance with subparagraph (A) shall not be considered to be valid by the recipient of such subpoena.

"(d) PROVISION OF CERTAIN INFORMATION TO ATTORNEY GENERAL.—

"(1) IN GENERAL.—Notwithstanding section 2245(a)(5) and paragraph (b)(2) of this section, if the Director determines, based on the information provided in response to a subpoena issued pursuant to subsection (c), that the facts relating to the cyber incident or ransom payment at issue may constitute grounds for a regulatory enforcement action or criminal prosecution, the Director may provide such information to the Attorney General or the head of the appropriate Federal regulatory agency, who may use such information for a regulatory enforcement action or criminal prosecution.

"(2) CONSULTATION.—The Director may consult with the Attorney General or the head of the appropriate Federal regulatory agency when making the determination under paragraph (1).

''(e) CONSIDERATIONS.—When determining whether to exercise the authorities provided under this section, the Director shall take into consideration—

''(1) the complexity in determining if a covered cyber incident has occurred; and

''(2) prior interaction with the Agency or awareness of the covered entity of the policies and procedures of the Agency for reporting covered cyber incidents and ransom payments.

''(f) EXCLUSIONS.—This section shall not apply to a State, local, Tribal, or territorial government entity.

''(g) REPORT TO CONGRESS.—The Director shall submit to Congress an annual report on the number of times the Director—

''(1) issued an initial request for information pursuant to subsection (b);

''(2) issued a subpoena pursuant to subsection (c); or

''(3) referred a matter to the Attorney General for a civil action pursuant to subsection (c)(2).

''(h) PUBLICATION OF THE ANNUAL REPORT.—The Director shall publish a version of the annual report required under subsection (g) on the website of the Agency, which shall include, at a minimum, the number of times the Director—

''(1) issued an initial request for information pursuant to subsection (b); or

''(2) issued a subpoena pursuant to subsection (c).

''(i) ANONYMIZATION OF REPORTS.—The Director shall ensure any victim information contained in a report required to be published under subsection (h) be anonymized before the report is published.

''SEC. 2245. INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.

''(a) DISCLOSURE, RETENTION, AND USE.—

''(1) AUTHORIZED ACTIVITIES.—Information provided to the Agency pursuant to section 2242 or 2243 may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

''(A) a cybersecurity purpose;

''(B) the purpose of identifying—

''(i) a cyber threat, including the source of the cyber threat; or

''(ii) a security vulnerability;

''(C) the purpose of responding to, or otherwise preventing or mitigating, a specific

threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or use of a weapon of mass destruction;

''(D) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

''(E) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a cyber incident reported pursuant to section 2242 or 2243 or any of the offenses listed in section 105(d)(5)(A)(v) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(d)(5)(A)(v)).

''(2) AGENCY ACTIONS AFTER RECEIPT.—

''(A) RAPID, CONFIDENTIAL SHARING OF CYBER THREAT INDICATORS.—Upon receiving a covered cyber incident or ransom payment report submitted pursuant to this section, the Agency shall immediately review the report to determine whether the cyber incident that is the subject of the report is connected to an ongoing cyber threat or security vulnerability and where

applicable, use such report to identify, develop, and rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures.

''(B) PRINCIPLES FOR SHARING SECURITY VULNERABILITIES.—With respect to information in a covered cyber incident or ransom payment report regarding a security vulnerability referred to in paragraph (1)(B)(ii), the Director shall develop principles that govern the timing and manner in which information relating to security vulnerabilities may be shared, consistent with common industry best practices and United States and international standards.

''(3) PRIVACY AND CIVIL LIBERTIES.—Information contained in covered cyber incident and ransom payment reports submitted to the Agency pursuant to section 2242 shall be retained, used, and disseminated, where permissible and appropriate, by the Federal Government in accordance with processes to be developed for the protection of personal information consistent with processes adopted pursuant to section 105 of the Cybersecurity Act of 2015 (6 U.S.C. 1504) and in a manner that protects per-

sonal information from unauthorized use or unauthorized disclosure.

''(4) DIGITAL SECURITY.—The Agency shall ensure that reports submitted to the Agency pursuant to section 2242, and any information contained in those reports, are collected, stored, and protected at a minimum in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199, or any successor document.

''(5) PROHIBITION ON USE OF INFORMATION IN REGULATORY ACTIONS.—

''(A) IN GENERAL.—A Federal, State, local, or Tribal government shall not use information about a covered cyber incident or ransom payment obtained solely through reporting directly to the Agency in accordance with this subtitle to regulate, including through an enforcement action, the activities of the covered entity or entity that made a ransom payment, unless the government entity expressly allows entities to submit reports to the Agency to meet regulatory reporting obligations of the entity.

''(B) CLARIFICATION.—A report submitted to the Agency pursuant to section 2242 or 2243

may, consistent with Federal or State regulatory authority specifically relating to the prevention and mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to such systems.

''(b) PROTECTIONS FOR REPORTING ENTITIES AND INFORMATION.—Reports describing covered cyber incidents or ransom payments submitted to the Agency by entities in accordance with section 2242, as well as voluntarily-submitted cyber incident reports submitted to the Agency pursuant to section 2243, shall—

''(1) be considered the commercial, financial, and proprietary information of the covered entity when so designated by the covered entity;

''(2) be exempt from disclosure under section 552(b)(3) of title 5, United States Code (commonly known as the 'Freedom of Information Act'), as well as any provision of State, Tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records;

''(3) be considered not to constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection; and