EXPLANATORY STATEMENT

Issued by authority of the Minister for Home Affairs

Security of Critical Infrastructure Act 2018

Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022

1 The instrument is made under section 61 of the *Security of Critical Infrastructure Act 2018* (the Act). The instrument commences on the day after registration on the Federal Register of Legislation, and is a legislative instrument for the *Legislation Act 2003* (the Legislation Act).

Purpose

2 Part 2 of the Act provides that the Secretary of the Department must keep a private Register of Critical Infrastructure Assets containing information in relation to those assets. Under Part 2, the responsible entity for a critical infrastructure asset must give operational information, and a direct interest holder in relation to the asset must give interest and control information, to the Secretary to be included in the Register.

3 Section 18A of the Act provides that Part 2 of the Act applies to:

- an asset specified in the rules (paragraph (1)(a)); and
- an asset that has been privately declared to be a critical infrastructure asset under section 51 of the Act, where the declaration determines that Part 2 applies to the asset (paragraph (1)(b)); and
- an asset that was a critical infrastructure asset immediately before the commencement of section 18A of the *Security Legislation Amendment (Critical Infrastructure) Act 2021* (the Amendment Act) (paragraph (1)(c)).

4 Part 2B of the Act provides that if a cyber security incident has a relevant impact on a critical infrastructure asset, a responsible entity for the asset to which that Part applies is required to give a relevant Commonwealth body a report about the incident.

5 Section 30BB of the Act provides that Part 2B of the Act applies to:

- an asset specified in the rules (paragraph (1)(a)); and
- an asset that has been privately declared to be a critical infrastructure asset under section 51 of the Act, where the declaration determines that Part 2B applies to the asset (paragraph (1)(b)).

6 Part 2 and Part 2B of the Act constitute 'positive security obligations' for responsible entities for critical infrastructure assets. The purpose of these rules is to specify that the obligations in Part 2 and Part 2B of the Act are 'switched on' for the critical infrastructure assets that are specified in the instrument.

7 The rules also provide a grace period of 6 months for the commencement of obligations under Part 2 and 3 months for the commencement of obligations under Part 2B.

Details of the instrument

8 Details of the instrument are included at **Attachment A**.

Consultation

9 An exposure draft of the instrument and associated explanatory statement was released for public consultation under sections 18AA and 30BBA of the Act in December 2021.

10 In December 2021, the Department posted to its website an exposure draft of the instrument and additionally emailed 750 entities who were identified as potential responsible entities for critical infrastructure assets that may be subject to Part 2B of the Act. The Department also advised relevant responsible entities that their asset may be additionally required to provide ownership and operational information to the Register of Critical Infrastructure Assets under Part 2 of the Act. Consultation on the Application Rules, which commenced on 15 December 2021, closed on 1 February 2022 and 36 submissions were received. All 36 submissions were reviewed and considered in the making of the Application Rules.

11 The regulatory impact of making the instrument was assessed in the regulatory impact statement attached to the Explanatory Memorandum to the Security Legislation Amendment (Critical Infrastructure) Bill 2020. That statement identified that compliance with the mandatory cyber incident reporting obligation has an average annual compliance burden of $242.89 per small entity, $681.19 per medium entity and $1,119.49 per large entity.

Parliamentary scrutiny etc.

12 The instrument is subject to disallowance under section 42 of the Legislation Act. A Statement of Compatibility with Human Rights has been prepared in relation to the instrument, and provides that to the extent that the instrument impacts human rights, the impact is reasonable and proportional. The Statement is included at **Attachment B** to this explanatory statement.

13 The instrument was made by Karen Andrews, Minister for Home Affairs, in accordance with sections 18A, 30BB and 61 of the Act.

Attachment A

Details of the *Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022*

Section 1 Name

This section provides that the name of the instrument is the *Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022* (the instrument).

Section 2 Commencement

This section provides that the instrument commences on the day after registration on the Federal Register of Legislation.

Section 3 Definitions

Section 3 sets out definitions of terms used in this instrument by reference to their definitions in the *Aviation Transport Security Act 2004* (ATSA), *Aviation Transport Security Regulations 2005* and the *Customs Act 1901*. The definitions of those terms will apply as amended from time to time by operation of paragraph 13(1)(b) of the *Legislation Act 2003* (the Legislation Act).

Section 4 Application of Part 2 of the Act

Subsection 4(1) of the instrument provides that Part 2 of the *Security of Critical Infrastructure Act 2018* (the Act) applies to the critical infrastructure assets specified in paragraphs (a) to (m) but excluding the assets mentioned in subsection (2).

Paragraphs 4(1)(1) and (m) of the instrument specify that Part 2 of the Act applies to critical electricity assets and critical gas assets that were not critical infrastructure assets prior to the commencement of section 18A of the Act. This is to ensure that Part 2 of the Act applies to assets that newly become a critical electricity asset or a critical gas asset as a result of the amendments made to the Act by the *Security Legislation Amendment (Critical Infrastructure) Act 2021* (the Amendment Act) and the subsequent implementation of the *Security of Critical Infrastructure (Definitions) Rules 2021* (the Definitions Rules).

It should be noted that paragraph 18A(1)(c) of the Act provides that Part 2 of the Act continues to apply to critical infrastructure assets that were critical infrastructure assets immediately before the commencement of section 18A. For this reason, Part 2 of the Act continues to apply to:

- critical electricity assets and critical gas assets that were already critical infrastructure assets immediately prior to the commencement of section 18A;
- critical water assets;
- critical port assets;
- an asset privately declared under section 51 before the commencement of section 18A of the Amendment Act.

As a result of being specified in subsection 4(1), the responsible entities for these assets have an ongoing obligation to give operational information, and direct interest holders an obligation to give interest and control

information, to the Secretary and to notify the Secretary of notifiable events (see sections 23 and 24 of the Act in particular).

Subsection 4(2) lists four specific sugar mills that are owned or operated by specified entities as excluded from the obligation to comply with Part 2 of the Act. Sugar mills owned or operated by these entities may fall within the definition of 'critical electricity asset' under section 10 of the Act and the Definitions Rules. The electricity generators run by The Haughton Sugar Company Pty Ltd, Pioneer Sugar Mills Pty Ltd, Mackay Sugar Ltd and MSF Sugar Pty Ltd are non-scheduled, seasonal generators, and would be unlikely to impact the electricity network in any significant way if they were unavailable so it is appropriate to exclude from the definition.

Subsection 4(3) outlines a grace period for compliance with Part 2 of the Act. Under this provision, Part 2 of the Act does not apply to the critical infrastructure assets mentioned in subsection (1) in the period beginning at the time that the asset becomes a critical infrastructure asset and ending the later of 6 months after the commencement of this instrument and 6 months after the instrument becomes a critical infrastructure asset. For example, if an asset becomes a critical infrastructure asset on 1 April, the obligations in Part 2 will generally apply from the following 1 October.

At the time of commencement of this instrument, the time that an asset becomes a critical infrastructure asset may be determined by reference to the commencement of:

- Schedule 1 to the Amendment Act (which inserted the definitions of the terms specified in subsection (1)); or
- the Definitions Rules (which prescribe detail relating to the definition of terms specified in subsection (1)).

The 6 month 'grace period' set out in subsection 4(3) for obligations under Part 2 of the Act does not apply to assets that were already critical infrastructure assets prior to the commencement of section 18A of the Act.

Section 5 Application of Part 2B of the Act

Subsection 5(1) of the instrument provides that Part 2B of the Act applies to the critical infrastructure assets specified in paragraphs (a) to (t) but excluding the assets mentioned in subsections (3) and (4).

Paragraph (1)(p) specifies that Part 2B of the Act applies to a critical aviation asset mentioned in subsection (2). Subsection 5(2) lists a number of particular assets that are critical aviation assets. The use of the word 'Australian' in paragraph 5(2)(b) means that this provision is not intended to include international airlines, but is intended to include domestic (Australian) airlines that conduct international operations in addition to their domestic routes.

As a result of being specified in subsection 5(1), the responsible entities for these assets have an obligation to notify the relevant Commonwealth body about critical cyber security incidents within 12 hours (see section 30BC of the Act) or of other cyber security incidents within 72 hours (see section 30BD).

Subsection 5(3) lists four specific sugar mills that are owned or operated by specified entities as excluded from the obligation to comply with Part 2 of the Act. Sugar mills owned or operated by these entities may fall within the definition of 'critical electricity asset' under section 10 of the Act and the Definitions Rules. The electricity generators run by The Haughton Sugar Company Pty Ltd, Pioneer Sugar Mills Pty Ltd, Mackay Sugar Ltd and MSF Sugar Pty Ltd are non-scheduled, seasonal generators, and would be unlikely to impact

the electricity network in any significant way if they were unavailable so are appropriate to exclude from the definition.

Subsection 5(4) will exclude certain assets from the requirement to comply with Part 2B of the Act after the passage of the Transport Security Amendment (Critical Infrastructure) Bill 2022 (the TSACI Bill). The TSACI Bill would make amendments to the ATSA and the *Maritime Transport and Offshore Facilities Security Act 2003* (MTOFSA) to create a cyber incident reporting obligation in the legislation that is tailored and fit-for-purpose for the aviation and maritime transport sectors.

Parts 1 of Schedule 3 to the TSACI Bill would make consequential amendments to the Act to replace the definition of 'critical aviation asset'. Part 2 of Schedule 3 of the TSACI Bill will make consequential amendments to the Act to repeal the definition of 'critical port asset' and to insert a new definition of 'critical maritime asset'. Subsection 5(4) of the instrument will mean that those assets, who will be subject to the cyber incident reporting regimes under the ATSA and MTOFSA if the TSACI Bill passes the Parliament, will be automatically excluded from the obligation to also provide a mandatory cyber incident report under Part 2B of the Act.

Subsection 5(5) of the instrument provides that Part 2B of the Act does not apply to the critical infrastructure assets specified in subsection (1) in the period beginning when the asset becomes a critical infrastructure asset, and ending at the later of:

- 3 months after the commencement of this instrument; and
- 3 months after the asset became a critical infrastructure asset.

Attachment B

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

Security of Critical Infrastructure (Application) Rules 2022 (LIN 22/026)

This Disallowable Legislative Instrument is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of the Disallowable Legislative Instrument

1 The *Security of Critical Infrastructure Act 2018* (the Act) contains positive security obligations intended to enhance the Government and industry's understanding of the threat environment faced by Australia's critical infrastructure, and build cyber situational awareness. The positive security obligations comprise of two aspects: reporting to the Register of Critical Infrastructure Assets (the Register) and mandatory cyber incident reporting.

2 The *Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022* (the Application Rules) prescribe the circumstances in which specified critical infrastructure assets are required to:

- provide ownership and operational information to the Register under Part 2 of the Act; and
- provide reports about cyber incidents to the Australian Cyber Security Centre (ACSC) under Part 2B of the Act.

3 To avoid doubt, each aspect of the positive security obligations will only apply once a rule is made in relation to that aspect for a critical infrastructure asset or class of critical infrastructure assets. The rules prescribe which aspects are 'switched on' for a critical infrastructure asset or class of critical infrastructure assets.

4 Under section 18A of Part 2 of the Act, direct interest holders and responsible entities for critical infrastructure assets are required to report ownership and operational information to the Register if any of the following apply:

- the asset is specified in the Application Rules (paragraph (1)(a))
- the asset is the subject or a declaration under section 51, and the declaration determines that this Part applies to the asset (paragraph (1)(b)), or
- immediately before the commencement of section 18A of the Act, the asset was a critical infrastructure asset (within the meaning of the Act prior to these amendments commencing) (paragraph (1)(c)).

5 Operational information is defined in section 7 of the Act as the information that a responsible entity, or an operator of the asset must provide to the Register in accordance with Part 2, Division 3 of the Act.

This information is being collected to assist in the Government's understanding of who is in a position to influence the control and operation of critical infrastructure assets.

6 Paragraph 18A(1)(a) of the Act, given effect by the Application Rules, effectively works as an 'on switch' through which the Minister can ensure that the reporting obligations only apply in appropriate situations. For example, the Minister may choose not to apply Part 2 to a class of critical infrastructure assets, if the information that would be provided under the obligations is already available to government through other means and therefore the desired security objectives are being achieved. Importantly, this will be used to avoid duplicate reporting to Government and thus reduce regulatory burden.

7 Paragraph 18A(1)(b) provides that assets declared to be critical infrastructure assets under section 51 of the Act will be subject to Part 2 if the declaration determines that Part 2 applies to the asset, noting the private nature of those declarations due to the associated security vulnerabilities. This ensures responsible entities of assets declared under section 51 are aware of their obligations under Part 2 without disclosing the identity of these sensitive assets.

8 Paragraph 18A(1)(c) of the Act, given effect by the Application Rules, also provides a transitional provision to ensure the obligations in Part 2 will continue to apply, uninterrupted, in relation to those critical infrastructure assets that had existing obligations under the Part immediately prior to the commencement of section 18A of the Act.

9 Under Part 2B of the Act, responsible entities of specified critical infrastructure assets will be required to report cyber security incidents to the relevant Commonwealth body. Collecting this information will support the development of an aggregated threat picture to inform both proactive and reactive cyber response options – from providing immediate assistance to working with industry to uplift broader security standards

10 Section 30BB of the Act provides that the mandatory notification requirements in Part 2B apply to a critical infrastructure asset if:

- the asset is specified in rules (Application Rules) made by the Minister under section 61 of the Act (paragraph (1)(a)), or

- the asset is subject to a declaration under section 51 of the Act (which enables the Minister to make a private declaration that an asset is a critical infrastructure asset) and the declaration under section 51 determines that Part 2B applies to the asset (paragraph (1)(b)).

11 This effectively works as an 'on switch' through which the Minister can ensure that this particular aspect of the positive security obligations only applies in appropriate situations.

12 Similar to new section 18A of the Act, this section allows for a nuanced, sector-specific or asset-specific approach to be taken on the application of this obligation in new Part 2B. In determining whether to make rules to apply the obligations under Part 2B to certain critical infrastructure assets, the Minister is likely to consider the appropriateness of any existing arrangements or requirements for responsible entities of those assets to report to Government or regulators the occurrence of a cyber-security incident or incidents, or other arrangements to provide the required visibility of the threat environment. If existing arrangements are deemed to be appropriate and effective, the Minister is unlikely to activate the reporting requirements in relation to the relevant critical infrastructure assets.

13 A note to sections 18A and 30BB indicates that specification by class is permitted by way of subsection 13(3) of the *Legislation Act 2003*. This subsection relevantly provides that a power to make a legislative instrument specifying a matter may identify the matter by referring to a class or classes of matters. This note has been included to clarify that the Minister has the discretion to specify in rules that Part 2 and Part 2B applies to:

- all critical infrastructure assets,
- a category of critical infrastructure assets such as critical broadcasting assets,
- a subset of assets within a category of critical infrastructure assets, such as liquid fuel pipelines that are critical liquid fuel assets, or
- a specific asset that is a critical infrastructure asset.

14 Both sections 18A and 30BB provide for the ability to offer a delayed commencement or 'grace period' in the future when an entity becomes a critical infrastructure asset, allowing the entity a reasonable period to adjust their business.

Human rights implications

15 This Disallowable Legislative Instrument engages the following human rights:

- the right to an adequate standard of living, including the right to adequate food in Article 11 of the *International Covenant on Economic, Social and Cultural Rights* (ICESCR);
- the right to the enjoyment of the highest attainable standard of physical and mental health, including medical service and attention in the event of sickness in Article 12 of the ICESCR; and
- the right to privacy in Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR).

The right to an adequate standard of living, including the right to adequate food

16 Article 11 of the ICESCR provides for the right of everyone to an adequate standard of living, including adequate food. Article 11 commits States Parties to the Covenant to improve methods of production and distribution of food.

17 Direct interest holders and responsible entities for critical infrastructure assets specified in the Application Rules will be required to report ownership and operational information to the Register to which Part 2 of the Act applies. Information obtained will inform the Government and industry's understanding of who has influence and control over infrastructure that is critical to the provision of essential services and supplies that maintain and sustain life throughout Australia. This includes, but is not limited to, food and grocery, and freight services.

18 Responsible entities for critical infrastructure assets specified in the Application Rules will also be required to report cyber security incidents to which Part 2B of the Act applies. Information obtained through cyber incident reporting will enable the Government to identify and rapidly respond to emerging threats.

19 Overall, an enhanced understanding of the evolving threat environment will improve the Government's ability to work with industry to reduce the likelihood of a disruption to distribution networks and other key operations of Australia's major supermarkets, which could impact the availability of critical food and groceries.

The right to the enjoyment of the highest attainable standard of physical and mental health

20 Article 12 of the ICESCR provides for the right of everyone to the enjoyment of the highest attainable standard of health. The United Nations Committee on Economic, Social and Cultural Rights has stated that the right to health embraces a wide range of socio-economic factors that promote conditions in which people can lead a healthy life, and extends to the underlying determinants of health.

21 Hospitals are crucial to Australia's ability to fulfil this obligation as they provide critical care for patients with a variety of medical, surgical and trauma conditions, and are therefore integral to the sustainment of life.

22 The Application Rules require responsible entities of critical hospitals, and other specified critical infrastructure assets with a high degree of interdependency with critical hospitals (such as assets within the energy sector), to report ownership and operational information to the Register and report cyber security incidents to the ACSC.

23 An enhanced understanding of the evolving threat environment will improve the Government's ability to work with industry to reduce the likelihood of a disruption to health and medical services that are essential for promoting the highest attainable standard of physical and mental health within Australia.

Right to privacy

24 Article 17 of the ICCPR provides that no one shall be subjected to arbitrary or unlawful interference with their privacy. Interferences with privacy may be permissible provided that where it is authorised by law and is not arbitrary. For an interference with the right to privacy not to be arbitrary, the interference must be for a reason consistent with the provisions, aims and objectives of the ICCPR and be reasonable in the particular circumstances. The United Nations Human Rights Committee has interpreted 'reasonableness' in this context to mean that 'any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case'.

25 The term unlawful means that no interference can take place except as authorised under domestic law.

26 The Application Rules may engage the right to privacy in relation to:

- responsible entity (owners or operators) for an asset
- the responsible entity's employees, or
- the responsible entity's customers/consumers.

27 For critical infrastructure assets specified in the Application Rules, responsible entities will be required to report ownership and operational information to the Register and cyber incidents to the ACSC. This will allow certain powers to be used in relation to those prescribed assets, and may engage the right to privacy of the asset's responsible entity, employees or customers. Such information is held securely by the Government and will not be made available on a public register.

Responsible entities

28 In 'switching on' the obligations under the Act for a critical infrastructure asset that is an individual, the following measures may engage the right to privacy under Article 17 of the ICCPR:

- mandatory notification of cyber-security incidents (Part 2B of the Act); and
- the obligation of a reporting entity for a critical infrastructure asset to give information and notify of events for the Register of Critical Infrastructure Assets (Part 2, Division 2 of the Act).

Register of Critical Infrastructure Assets – obligations to give information and notify of events

29 Whilst the collection of personal information will be rare, Part 2 of the Act requires the responsible entity of critical infrastructure assets to provide the Secretary of the Department administering the Act with certain interest and control information in relation to the entity and the asset, which is maintained in a Register.

30 The requirements for the Register may result in the incidental collection of personal information in relation to responsible entities who are individuals. The responsible entity for specified critical infrastructure assets is required to provide high-level information on who ultimately controls or influences an asset though ownership, including beneficial ownership, or through operation arrangements, such as outsourcing arrangements.

31 The Register is used by the Government to prioritise and inform risk assessments to identify and manage national security risks in critical infrastructure assets. The interest and control information and operational information on the Register provides the Government with a more comprehensive understanding of how the asset and sector operates, and where there may be vulnerabilities. The information on the Register also influences the Government's ability to develop strategies to mitigate or reduce national security risk for assets which, if disrupted, would significantly impact the operations of large population hubs, economic interests and government operations.

32 The Government has taken sufficient steps to ensure that the limitations on the right to privacy are no more restrictive than necessary as the use and disclosure of information on the Register is restricted to purposes authorised under the Act. All information obtained under the Act, including the information provided for the Register, is protected information. It is a criminal offence to use or disclose protected information other than as authorised by Part 4, Division 3 of the Act. This Division enables disclosure for national security, foreign investment in Australia, taxation policy, industry policy, defence purposes or to assist regulatory bodies with oversight of any relevant industry for the critical infrastructure asset. Part 4, Division 3, Subdivision B of the Act provides criminal penalties to deter the disclosure of protected information.

33 The information on the Register may be shared with the relevant states and territories. This information may have broader policy implications for states and territories, particularly in relation to maintaining the security and resilience of critical infrastructure assets vital for their jurisdiction. This acknowledges that the states and territories, as owners and regulators of critical infrastructure assets share the responsibility with the Government to manage national security risks.

34 Further, safeguards for the protection of personal information specified in the Australian Privacy Principles (APP) under the *Privacy Act 1988* will apply to interest and control information, and operational information gathered under Part 2, and Part 2B of the Act. This includes requirements

regarding the security of personal information specified under APP 11 and requirements regarding use or disclosure under APP 6.

35 To the extent that the Register may result in the incidental collection of personal information and limit the right to privacy in Article 17, this limitation is permissible as the collection of personal information would be lawful, would not be arbitrary and would be reasonable, necessary and proportionate to achieving a legitimate national security objective.

Secretary's powers to obtain information or documents

36 The Secretary's information gathering power is a permissible limitation to the right to privacy. Subsection 37(1) of the Act empowers the Secretary to request certain information from reporting entities and operators of critical infrastructure assets. The Act allows for the Secretary to request information or documents that may be relevant to:

- the Secretary's duty and function to keep a Register under section 19
- the Minister's power to issue a direction under subsection 32(2),
- the Secretary's power to issue a direction under subsection 35AK(2), and
- the Secretary's power to undertake an assessment of a critical infrastructure asset to determine if there is a national security risk under section 57.

37 The information requested may include procurement plans, tender documentation, contracts, name and citizenship of board members and other documents specifying business operations. The notice may require the provision of personal information, which may limit the right to privacy.

38 The information gathering power is limited to obtaining information or documents that are directly relevant to the purposes of the legislation, as stated in the objects of the Act, as well as the functions, duties, powers and purposes prescribed in the Act. Any personal information collected is incidental to the key objective of developing a more detailed understanding of possible national security risks.

39 This power was drafted with reference to the Administrative Review Council's best practice principles for implementing and exercising information gathering powers in its 2008 report, *Coercive Information Gathering Powers of Government Agencies.*

40 In practice, Government agencies will also engage with the relevant entity prior to issuing a notice to discuss the nature of the information required and, if necessary, the terms of the notice. Engagement with the relevant entity will ensure that prior to issuing a notice a range of matters including the impact on the right of privacy will be considered. This ensures the Secretary's notice is a proportionate response, balancing the impacts on privacy with the Government's objective of addressing national security risks to critical infrastructure.

41 The information and documents provided to the Secretary in response to a request are protected information and the use and disclosure of the information is restricted in line with provisions at Part 4, Division 3 of the Act. This Division enables disclosure for national security, foreign investment in Australia, taxation policy, industry policy, defence purposes or to assist regulatory bodies with oversight of any relevant industry for the critical infrastructure asset. Part 4, Division 3, Subdivision B of the Act provides criminal penalties to deter the disclosure of protected information.

42 The information on the Register may be shared with the relevant states and territories. This acknowledges that the states and territories, as owners and regulators of critical infrastructure assets share the responsibility with the Government to manage national security risks.

43 Further, safeguards for the protection of personal information specified in the Australian Privacy Principles (APP) under the *Privacy Act 1988* will apply to interest and control information, and operational information gathered under Part 2, and Part 2B of the Act. This includes requirements regarding the security of personal information specified under APP 11 and requirements regarding use or disclosure under APP 6.

44 To the extent that the Secretary's information gathering powers may result in the incidental collection of personal information and limit the right to privacy in Article 17, this limitation is permissible as the collection of personal information would be lawful, would not be arbitrary and would be reasonable, necessary and proportionate to achieving a legitimate national security objective

Conclusion

The Disallowable Legislative Instrument is compatible with human rights because it promotes human rights and, to the extent that it may limit human rights, those limitations are reasonable, necessary and proportionate to the objective of reducing national security risks, including those presented by cyber threats, to critical infrastructure.