

Security in Grant NOFO Checklist

Can you commit to report to the Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) cybersecurity incidents involving systems that you operate and maintain including:

- 1) Unauthorized access of an Information or Operational Technology system;
- 2) Discovery of malicious software on an Information or Operational Technology system;
- 3) Activity resulting in a denial of service to any Information or Operational Technology system;
- 4) A physical attack against network infrastructure, such as deliberate damage to communication lines; and
- 5) Any other cybersecurity incident that results in operational disruption to the Information or Operational Technology systems or other aspects of the pipeline systems or facilities, or otherwise has the potential to cause operational disruption that adversely affects the safe and efficient transportation of natural gas including, but not limited to impacts to a large number of customers, critical infrastructure or core government functions, or impacts national security, economic security or public health and safety.

Can you commit to report this information required as soon as practicable after a cybersecurity incident is identified?

- Reports must be made to CISA Central using CISA's Reporting System form at:
 - <https://us-cert.cisa.gov/forms/report> or by calling (888) 282-0870.5 If the required information is not available at the time of reporting, you must submit an initial report within the specified timeframe and supplement as additional information becomes available. All reported information will be protected in a manner appropriate for the sensitivity and criticality of the information.
- Reports must be made to the local FBI field office, which can be found here: <http://www.fbi.gov/contact-us/field>

Transportation Security Administration (TSA) Pipeline Security Guidelines
(https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf)

- Have you reviewed the Guidelines?
- Are any of the facilities you operate identified as "critical?"
- Even if they are not considered "critical," have you thought about conducting a risk assessment to determine vulnerabilities?
- If you completed a risk assessment, have you determined what actions you need to take to mitigate risk?
- What is the status of those actions?

TSA Security Directive (SD) Pipeline-2021-02C

- Recognizing that this is only applicable for critical pipeline operators, have you read through the SD, specifically III. B. through III. E.? Any plans you can share on how your utility is meeting these requirements?