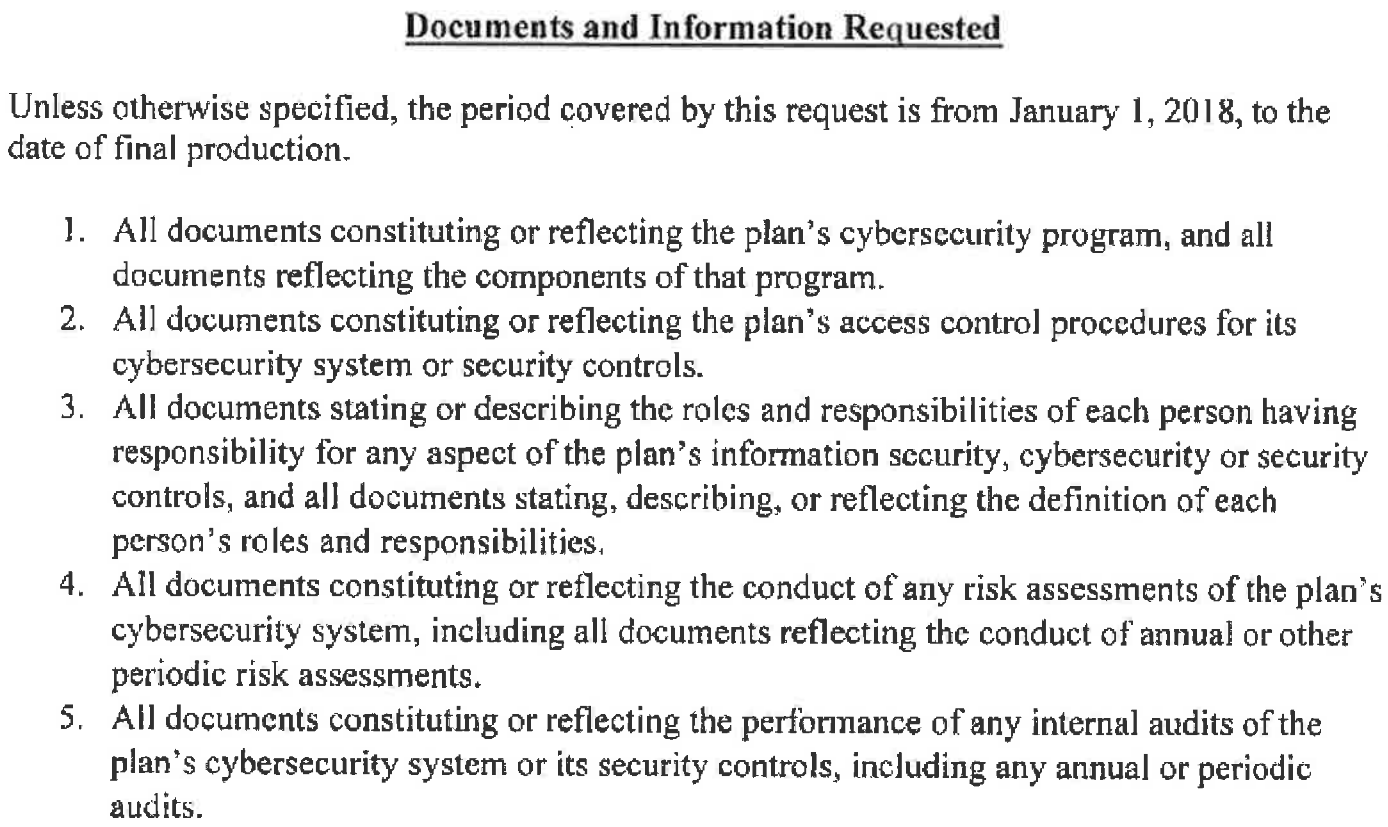
Example A – Cybersecurity Requests

- All policies, procedures or guidelines relating to:
  - Data governance, classification and disposal.
  - The implementation of access controls and identity management, including any use of multi-factor authentication.
  - The processes for business continuity, disaster recovery, and incident response.
  - The assessment of security risks.
  - Data privacy.
  - Management of vendors and third-party service providers, including notification protocols for cybersecurity events and the use of data for any purpose other than the direct performance of their duties.
  - Cybersecurity awareness training.
  - Encryption to protect all sensitive information transmitted , stored, or in transit.
- All documents and communications relating to any past cybersecurity incidents involving Plan accounts at the Plan Level or related Plan service providers.
- All security risk assessment reports.
- All documents describing security technical controls, including firewalls, antivirus software, and data backup.
- All documents and communications from service providers relating to their cybersecurity capabilities and procedures.

Example B--DOL Cybersecurity Document Requests



Documents and Information Requested

Unless otherwise specified, the period covered by this request is from January 1, 2018, to the date of final production.

1. All documents constituting or reflecting the plan's cybersecurity program, and all documents reflecting the components of that program.
2. All documents constituting or reflecting the plan's access control procedures for its cybersecurity system or security controls.
3. All documents stating or describing the roles and responsibilities of each person having responsibility for any aspect of the plan's information security, cybersecurity or security controls, and all documents stating, describing, or reflecting the definition of each person's roles and responsibilities.
4. All documents constituting or reflecting the conduct of any risk assessments of the plan's cybersecurity system, including all documents reflecting the conduct of annual or other periodic risk assessments.
5. All documents constituting or reflecting the performance of any internal audits of the plan's cybersecurity system or its security controls, including any annual or periodic audits.

Example B--DOL Cybersecurity Document Requests

6. All documents constituting or reflecting any third-party audits of the plan's cybersecurity system or its security controls, including any annual or periodic audits, performed by any outside party or entity.
7. All documents constituting or reflecting any security reviews and/or independent security assessments performed that relate to assets or data stored in a cloud or managed by a third-party service provider.
8. All documents constituting or reflecting the conduct of cybersecurity awareness training, including all periodic cybersecurity awareness training.
9. All documents constituting or reflecting any business resiliency program or business continuity program relating to the plan's cyber system or its cybersecurity, including processes for business continuity, disaster recovery, and incident response.
10. All documents reflecting the plan's implementation of technical controls for its cybersecurity program.

Example B--DOL Cybersecurity Document Requests

11. All documents constituting or reflecting the implementation and/or management of a secure system development life cycle (SDLC) program.
12. All documents reflecting the occurrence of any cybersecurity incidents, breaches, or suspected incidents or breaches, and the actions taken in response to each.
13. All documents constituting or reflecting the plan's processes for the encryption of sensitive data, stored and in transit.
14. All documents constituting or relating to any contracts with any third-party service providers that provide services relating to the plan's information security, cybersecurity, or security controls.