

Data Protection Plan Working Group

Report out to ACCRES

June 4, 2019

DISTRIBUTION STATEMENTS:

Unlimited.

EXPORT CONTROL STATEMENTS:

None.

Summary of Working Group Efforts

- The working group convened several times via telephone following the October 18, 2018 meeting of ACCRES.
- The Working Group was tasked with revising the Data Protection Plan Template for a second time to incorporate a two (2) class system replacing the previously proposed three (3) class system.
 - Formatting changes were also requested.
- The Working Group developed a draft Template and collaboratively made suggested edits and comments. Members also made recommendations regarding data protection.
- The draft was consolidated into a revised Template and forwarded to NOAA CRSRA and the ACCRES Chair for review.
- A Notice of Proposed Rule Making was published in the Federal Register on May 14, 2019. The NPRM reflects a substantial rewrite of existing regulations.
- The Requirement for a Data Protection Plan appears to be eliminated in the proposed rules and replaced in part by a Cybersecurity Framework document.

Recommendations

Modes of Operation

- It is recommended that licensees use NIST-approved modes of operation.
 - <https://csrc.nist.gov/Projects/Block-Cipher-Techniques/BCM/Current-Modes>

Modes of Operation

- It is recommended that licensees use NIST-approved authenticated encryption where both confidentiality and authentication is necessary.
 - Encryption alone does not guarantee authenticity

Modes of Operation

- It is recommended that NOAA permit the use of NIST-approved authentication to secure plain text commands, telemetry and data for private remote sensing systems using spectrum where encryption is prohibited and where confidentiality is not necessary
 - Enabling for amateur and student projects using amateur radio bands
 - GCM authenticated encryption mode of operation explicitly provides for *additional authenticated data* in addition to encrypted data, while authenticating them both with same level of security