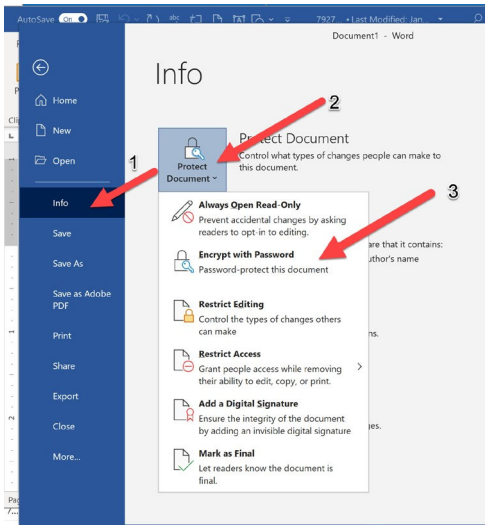
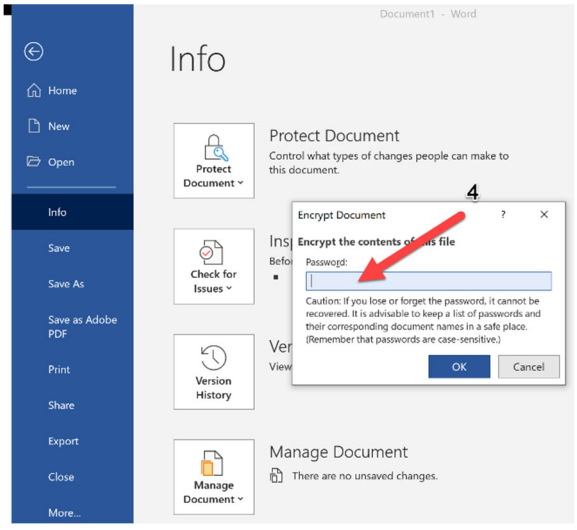
Procedure for the Secure Transmittal of Cybersecurity Plans

When it comes to sensitive documents like cybersecurity plans, steps should be taken to enable the security of these documents during transmittal and storage. Cybersecurity plans need to be securely transmitted to the DOE cybersecurity plan review team. The review team is required to store and review the cybersecurity plans and any associated documentation in a secure manner. Below is a procedure that selectees or recipients can use to securely transmit the cybersecurity plan and related attachments.

1) **Encrypt files:** Email attachments and other forms of file transmittal are generally not encrypted by default. To enhance the security of your cybersecurity plans during email transmission and the review process, it is recommended that you encrypt your cybersecurity plans.
    a. To encrypt Word files, here is a simple, easy-to-use approach:
        - Go to the "File" tab and click "Info" (Step 1)
        - Click the "Protect Document" item (Step 2)
        - Click the "Encrypt with Password" item (Step 3)
        - Enter a password then click OK, then re-enter the password and click OK (Step 4). The password does not have to overly long or complex, but a minimum of 8 characters and a combination of upper-case, lower-case, and numbers are recommended. Remember to record and store your password (e.g., in a logbook, in an electronic password safe) in a secure manner so that it can readily retrieved when needed.





After completing the above steps, the "Protect Document" item will change color and the associated message on the Info page will say, "*A password is required to open this document*".

b. For other types of documents (e.g., PDF files) similar encryption options should be available. Use that software's associated Help function to learn the steps need to encrypt the document.

2) **Check the size of the file(s)**: Some email providers have a limit on how large a message and its attachments can be and if the package is too big, the email might not go through. If your file or files are large (e.g., some email systems have issues with transmittals larger than 20MB), you may need to compress your original files (e.g., using Zip) or you may use a secure file transfer service for large files instead of email.

3) **Transmit the file:** Now that the document is encrypted with its own unique password, it can typically be transmitted as an email attachment or shared using a secure file transfer service. To enhance security, you have the option of adding end-to-end email encryption (e.g., using Entrust). Send the email to the following address CR-IIJACybersecurityplans@hq.doe.gov.

4) **Send the password securely**: Once the encrypted file has been transmitted, the password needs to be securely shared.

   a. Send a second email to CR-IIJACybersecurityplans@hq.doe.gov with a non-descript subject line that contains the password for the encrypted file that you sent. Never send both a password-protected file and its password in the same email. If both are in the same email, then an adversary can easily decrypt the sensitive file using the included password.

5) **Confirm delivery:** A verbal or written confirmation of the receipt and successful opening of your cybersecurity plan by the Cybersecurity team will be provided.