Describe the Benefits and Use Cases of Seal Wrapping

What is Seal Wrapping?

Vault already protects my data using 256-bit AES, but how I can provide an extra layer of protection while meeting FIPS 140-2 compliance?

- Seal Wrapping essentially provides "double encryption" by encrypting the data using keys stored on an HSM
- Provides FIPS 140-2 compliance* by integrating with an HSM
  - Supports the FIPS level equivalent to the HSM – so if you use a Level 3 HSM, you will be used Level 3 cryptography
- Allows Vault to be deployed in high-security GRC environments (PCI, HIPAA, DoD, NATO)

*Starting with v1.10.3, HashiCorp is now publishing Vault binaries that can provide FIPS 140-2 compliance without requiring an HSM integration

What is Seal Wrapped by Default?

- Recovery Key
- Any stored key shares
- The root key
- The keyring

What Can We Enable?

- Seal wrapping is enabled by default on supported seals
- Causes values stored by the mount to be wrapped by the seal's encryption capability
  - You can disable this by setting `disable_sealwrap=true` in the config file

- Backend mounts (secrets engines, etc.) can take advantage of seal wrapping as well
- When enabling a secrets engine, provide the `seal_wrap=true` configuration
  - CLI flag to enable seal wrap on a secrets engine: `-seal-wrap`

Enabling Seal Wrapping for Key/Value


```
# Enable a secrets engine with seal wrap
$ vault secrets enable -seal-wrap kv


# List the enabled secrets engines
$vault secrets list -detailed
Path          Plugin     Accessor                Seal Wrap
----          ------     --------                -----------
...
cubbyhole/    cubbyhole  cubbyhole_b36dd7e1      false
identity/     identity   identity_b5650a96       false
kv/           kv         kv_fe02767b             true
```