

ATTACHMENT A
Summary Chart on Controls for Electronic Information

Type	Definition	Control
I-PII	Data defined as PII by regulation or requirement	Data is only stored on network storage devices. Access is controlled by network credentials. Special authorization required for transportation on mobile devices. Users receive special training to ensure protection of this data.
I	Data that has been specifically defined as needing encryption by requirement such as Sensitive Unclassified Information	Data is stored or transported encrypted as required and, requires two factor authentication for remote access. Users receive special training to ensure protection of this data.
II	Business Sensitive Data – data that has a direct bearing on business decisions that if compromised could result in an unfair advantage to parties conducting business or in legal action with the department. Type II data is designated by the Content Owner	Data access is controlled through the network and requires two factor- authentications for remote access. Data is protected by encryption in transport.
III	Information about Business Sensitive Data that requires protection to ensure data integrity, and a level of confidentiality, or data needs to be screened from the general public. Type III data is designated by the Content Owner	Data access is controlled through the network, requires username and password for remote access. Files transported on removable media should be protected by password.
IV	Public data that may be released at any time. Web site data makes up the bulk of this data	Data access is controlled through the network. Data is posted to the web as directed by the Content Manager. Precautions are taken to ensure data integrity.