

Data Security Rules, Regulations and Standards

Before considering whether the US Postal Services Secure Destruction Mail Service conforms to or complies with any given data security regulation or standard, it is critically important that mailers fully understand what the SD mail service is and how it works. This will ultimately affect which rules and regulations apply and which do not. One of the core factors in making a determination of applicability for most all data security rules and regulations is “access” to “personally identifiable information (PII).” First class mail (FCM) by definition is a protected class of mail by law. Those protections are why the federal government, such as the US Department of State and the US Treasury, identify USPS FCM in their data security regulations as an acceptable method for transmitting “Secret,” “Highly Classified” and “Classified” information. The PII data that the SD mail service is designed to protect would fall under the lower “Confidential” classification per International Standard for Destruction DIN 66399 (see pg. 14).

When mailers sign up for SD Mail Service it is important to know that the USPS does not have access to the personally identifiable information (PII) contained within the mailpiece (i.e. hardcopy data). Also important to know, is any information transmitted electronically to the mailers or mail service providers does not contain PII (i.e. electronic data). Just like we do now with all first class mail, we only transmit mailpiece data taken from the front of the envelope using the mailer IMb located in the address block. Only the mailers know what their own unique numerical identifiers in IMb mean.

The United States Postal Service, as defined by law, is the government agency responsible for protecting the sanctity of the mail and we are tasked with regulating and enforcing how that is done. That is one of advantage that comes with using the USPS’s SD Mail Service. USPS mailers, from the government, financial, healthcare, insurance, utility, telecommunications, educational, retail, and legal industries that use the SD Mail Service, do not have to self-regulate a *Service Provider, Third Party Handler, Business Associate* and the like to prove they are compliant with the applicable data security rules and regulations for those industries.

In the following, we will provide some specific examples of how the data security standards, rules and/or regulations do not apply to the *SD Mail Service Option* available to USPS mailers.

HealthCare Industry - The [Health Insurance Portability and Accountability Act \(HIPAA\)](#) was established in 1996 to improve the healthcare system’s storage and use of patient data. In the service of making healthcare insurance safer and more reliable for everyone, Congress recognized the need to secure patients’ personal information and regulate its disclosure. Per this mission, the [Privacy Rule](#) and [Security Rule](#) under HIPAA apply to all protected health information (PHI) and guide the measures needed to guard the privacy and integrity of health data in the digital age.

Before reviewing the law itself, it's helpful to know what organizations are responsible for implementing HIPAA standards. [Covered Entities \(CE\)](#) under HIPAA include healthcare providers, health plans, and healthcare clearinghouses. Most components of HIPAA also apply to any [Business Associate \(BA\)](#) of a covered entity. A Business Associate (BA) is any third party who handles protected health information (PHI) in providing a service for a covered entity (CE). A BA, for example, could be an external administrator who processes claims or a CPA firm that must access protected data to execute its accounting services.

In regards to the HIPAA definition of "Covered Entities (CE)," it does not apply to the USPS or the SD Mail Services provided by the USPS. The other responsible organization definition under HIPAA is "Business Associate (BA)." SD Mail Service does not involve any handling of protected health information (PHI). The mailer's customer PHI is secured within the mailpiece and is not accessible to the USPS. Therefore the USPS also does not fall under the HIPAA definition of "Business Associate (BA)." In summary, HIPAA does not apply to the *USPS SD Mail Service* and actually goes onto exempt the US Postal Service in the Security Rule (see below).

Excerpt from the HIPPA Security Rule

Other Situations in Which a Business Associate (BA) Contract Is "NOT" Required.

*With a person or organization that acts merely as a conduit for protected health information, **for example, the US Postal Service**, certain private couriers, and their electronic equivalents.*

Financial Industry - The **Payment Card Industry (PCI) Security Standards Council** was originally formed by American Express, Discover Financial Services, JCB International, MasterCard and Visa Inc. on September 7th, 2006 with the goal of managing the ongoing evolution of the Payment Card Industry Data Security Standard (PCI DSS). The council operates as an entity independent of the various card vendors that make up the council. The Payment Card Industry Data Security Standard (PCI DSS) established by the council, consist of twelve significant requirements including multiple sub-requirements which contain numerous directives against which businesses may measure their own payment card security policies, procedures and guidelines.

As a global standard, **the PCI DSS applies to any entity worldwide that stores, processes or transmits credit cardholder data.** This includes financial institutions, merchants and **service providers** in all payment channels.

- Financial institutions include banks, insurance companies, lending agencies, and brokerages.
- Merchants include restaurants, retailers (brick-and-mortar, mail/telephone order, e-commerce), transportation operators, and virtually any point-of-sale that processes credit cards across all industries.

- Examples of service providers include transaction processors, payment gateways, customer service entities, (i.e. call centers), managed service providers, web hosting providers, data centers, and Independent Sales Organizations.

The five major payment card brands enforce PCI compliance validation by requiring merchant banks to meet specific auditing and reporting criteria for their respective merchants and service providers.

Per the PCI DSS description of an “applicable entity” and “service provider” noted above, it is important to know that USPS mail services, including SD Mail Service, **do not involve any storage, processing or transmittal of credit cardholder data**. This data is securely contained within each mailpiece throughout the entire process. In summary, **the PCI DSS standard does not apply to the USPS SD Mail Service**.

The PCI DSS also emphasizes the importance of evaluating **RISK**. Risk is calculated many ways, but in each case it involves assessing the probability and the severity of the perceived risk. It is represented by the formula *Risk = Probability x Severity*.

Also when evaluating risk one needs to consider the current of baseline condition and compare it to the modified of alternative condition to determine if risk increases or decreases. If you apply these concepts to the SD mail services provided by the US Postal Service, mailers should first understand what is currently taking place and how they handling their first class RTS mail now. Things to consider include:

- 1) How many physical touch points are there in the entire process?
- 2) How much control do they have when it comes to managing their RTS mail?
- 3) Are third parties or service providers being used that also need to be managed per the PCI DSS?
- 4) What historical data is available to better define the potential probability and severity of the risk?

This will vary for each mailer, but we offer the following for consideration when comparing risk from your baseline/current condition to the alternative SD Mail Service option.

- 1) There are significantly fewer touch points involved with managing undeliverable SD mail.
- 2) Mailers RTS mail volume is significantly reduced, thus reducing mailer’s need to use 3rd parties or internal staff to handle RTS mail and data.
- 3) Mailers may lessen liabilities by using fewer service providers that are directly subject to the PCI DSS.
- 4) Fewer people and entities need to be involved with protecting the data contained in the undeliverable RTS mail.
- 5) Less oversight of service providers and/or staff should prove to be more manageable and controllable.

National Association of Information Destruction (NAID): NAID has become an influential force in promoting secure destruction industry standards and education, most notably in the United States. Many mailers who utilize third party service providers to handle and destroy their first class RTS mail require that these entities be NAID Certified. The Postal Service® carefully examined the NAID certification process for Secure Destruction and determined that it is not applicable to US Postal Service and would actually be in conflict with the USPS® regulatory mandate to protect the sanctity of mail. Voluntary compliance with the NAID certification process on behalf of The Postal Service® would not meet existing USPS® security standards and legal penalties under 18 USC. While NAID does not apply, the following *SD Mail Service vs. National Association for Information Destruction (NAID) Criteria Cross Comparison Table* provides mailers with a glimpse of what those differences are.

SD Mail Service vs. National Association for Information Destruction (NAID) Criteria* Cross Comparison Table

Item	NAID Criteria and USPS® Secure Destruction Strategy
1.1	<p>NAID Criteria: All Access Individuals and Non-Access Employees must sign a Confidentiality Agreement prior to gaining access to Confidential Customer Media and employees must be legally Registered to work at the Company:</p> <ul style="list-style-type: none"> ▪ Confidentiality Agreement ▪ I-9 for US employees hired after November 7, 1986 or proper work registration for non-citizens <p><i>Secure Destruction Strategy: USPS® exceeds this NAID standard per the hiring policies in EL 312. Moreover, US Mail is not opened by USPS® employees so there would not be any access to confidential materials in the mail.</i></p>
1.2	<p>NAID Criteria: Access Individuals* are subject to the employment screening restriction requirements of NAID Certification, including criminal background check, initial employment drug-screening and previous employment verification. Screening for Access Individuals* must include:</p> <ul style="list-style-type: none"> ▪ 7 Year Criminal Record Search: <ul style="list-style-type: none"> – Social Security Header Search (must be conducted prior to the criminal background investigation to ensure all states and counties of residence and employment have been included (and verified) in the investigation) – Federal Records Search for all Federal Districts in all states on SS Header Search – Statewide records search for all states on SS Header Search – County records search for all counties on SS Header Search ▪ Pre-hire or Initial Drug Screening ▪ 7 Year Employment History Verification must minimally include the following for each place of prior employment: <ul style="list-style-type: none"> – Name of the previous employer – Dates of employment, as reported by the employee – Date of verification (or attempted verification if the previous employer cannot be reached) – Indication of whether or not the previous employer was able to verify the dates of reported employment <p><i>Secure Destruction Strategy: USPS® exceeds this NAID standard as set forth in USPS® Handbook EL-312 which governs eligibility and screening standards for all new employees. There is no time limit on the criminal background search for prospective USPS® employees.</i></p>
1.2	<p>NAID Criteria: A Criminal Record Search must be conducted for each place of residence and employment during the previous 7 years and obtained through a third-party background search service. For all places in the U.S., federal, statewide and county-by-county searches must be conducted for any record searches conducted after January 1, 2012. Prior to that date, only statewide and county-by-county searches were required. If federal, statewide and/or county searches are not available in a particular state, the applicant may do the ones available and provide documentation to support the unavailability of the other. For all places in Canada, searches must be done on a province/territory and National basis and obtained through a third-party background search service or Canadian Police Information Centre (CPIC). When searches are being conducted in places outside of the U.S. every effort should be made to have the searches done at a level</p>

Item	NAID Criteria and USPS® Secure Destruction Strategy
	<p>comparable to the statewide and county-by-county searches done in the U.S. (See Employment Information Disclaimer.)</p> <p>Secure Destruction Strategy: USPS® does not exceed this NAID standard as set forth in USPS® Handbook EL-312, Section 5.14.33. The USPS® only reviews the place of residence for the last 5 years. However, the USPS® only hires citizens and lawful permanent resident aliens, which exceeds the NAID standards which do not have a United States focus.¹</p>
2.1c	<p>NAID Criteria: The Company has a written policy in place, stating that it will notify any Customer of a potential release of, or unauthorized access to, that Customer’s Confidential Customer Media that poses a threat to the security or confidentiality of that information within 60 days of the date of discovery of the data security breach incident.</p> <p>Secure Destruction Strategy: The USPS® has very strong controls over the unauthorized access to confidential materials with respect to mail as follows. For details see the USPS® Employee Labor Relations Manual. Instructions on mail security as it relates to unauthorized opening, inspection, tampering, or delay of mail are in Administrative Support Manual 274. In addition to the statutes listed in Title 5, Code of Federal Regulations (CFR), Part 2635.901-902, the following statutes and regulations are applicable to all employees in the Postal Service:</p> <ul style="list-style-type: none"> ▪ a. Prohibition against proscribed political activities (Title 5, United States Code (U.S.C.), subchapter III of chapter 73, and 18 U.S.C. 602, 603, 607, and 608) ▪ b. Prohibition against appointing or promoting a relative, or advocating such an appointment or promotion (5 U.S.C. 3110) ▪ c. Prohibition against disloyalty and striking (5 U.S.C. 7311; 18U.S.C.1918) ▪ d. Prohibition against bribery, graft, and conflicts of interest (18U.S.C.201, 203, 205, 208, and 209) ▪ e. Prohibition against acting as the agent for a foreign principal registered under the Foreign Agents Registration Act (18 U.S.C. 219) ▪ f. Prohibition against unauthorized taking or use of documents relating to claims against or by the government (18 U.S.C. 285) ▪ g. Prohibition against postal employees becoming interested in any contract for carrying the mail (18 U.S.C. 440) ▪ h. Prohibition against counterfeiting and forging transportation requests (18 U.S.C. 508) ▪ i. Prohibition against deprivation of employment or other benefit for political activity (18 U.S.C. 601) ▪ j. Prohibition against: <ul style="list-style-type: none"> - (1) Embezzlement of government money or property (18 U.S.C. 641) - (2) Failing to account for public money (18 U.S.C. 643) - (3) Embezzlement of money or property of another person in the possession of an employee by reason of his or her employment (18 U.S.C. 641) ▪ k. Prohibition against: <ul style="list-style-type: none"> - (1) Disclosure of classified information (18 U.S.C. 798) - (2) Disclosure of confidential information (18 U.S.C. 1905). • l. Prohibition against fraud or false statements in a government matter (18 U.S.C. 1001)

Item	NAID Criteria and USPS® Secure Destruction Strategy
	<ul style="list-style-type: none"> ▪ <i>m. Prohibition against participation in lottery enterprises (18 U.S.C. 130)</i> ▪ <i>n. Prohibition against carriage of mail contrary to law (18 U.S.C. 1693)</i> ▪ <i>o. Prohibition against desertion of mail (18 U.S.C. 1700)</i> ▪ <i>p. Prohibition against obstruction of correspondence (18 U.S.C. 1702)</i> ▪ <i>q. Prohibition against delay or destruction of mail or newspapers (18 U.S.C. 1703)</i> ▪ <i>r. Prohibition against theft of property (18 U.S.C. 1707)</i> ▪ <i>s. Prohibition against theft of mail (18 U.S.C. 1709).t. Prohibition against theft of newspapers (18 U.S.C. 1710)</i> ▪ <i>u. Prohibition against misappropriation of Postal Service funds (18 U.S.C. 1711)</i> ▪ <i>v. Prohibition against falsification of postal returns (18 U.S.C. 1712)</i> ▪ <i>w. Prohibition against improper issuance of money orders (18 U.S.C. 1713)</i> ▪ <i>x. Prohibition against misuse of the franking privilege (18 U.S.C. 1719)</i> ▪ <i>y. Prohibition against the unlawful sale or pledge of stamps (18 U.S.C. 1721)</i> ▪ <i>z. Prohibition against unlawful collection of postage (18 U.S.C. 1726)</i> ▪ <i>aa. Prohibition against improper approval of bond or sureties (18 U.S.C. 1732)</i> ▪ <i>ab. Prohibition against lobbying with appropriated funds (18 U.S.C. 1913)</i> ▪ <i>ac. Prohibition against the use of deceit in an examination or personnel action in connection with gov't employment (18 U.S.C. 1917)</i> ▪ <i>ad. Prohibition against mutilating or destroying a public record (18U.S.C.2071)</i> ▪ <i>ae. Prohibition against disclosure of lists of names and addresses (39U.S.C. 412)</i> ▪ <i>af. Prohibition against making or receiving political recommendations for appointment or promotion (39 U.S.C. 1002)</i> ▪ <i>ag. Prohibition against receipt of unauthorized fees (39 U.S.C. 1009)</i> ▪ <i>ah. Prohibition against opening First-Class Mail® (39 U.S.C. 3623)</i> ▪ <i>ai. Oath of office required for all postal employees (39 U.S.C. 1011)</i> ▪ <i>aj. Privacy Act of 1974 (5 U.S.C. 552a)</i>
2.1d.	<p>NAID Criteria: The Company has a written policy in place instructing and requiring employees to notify management of a potential release of, or unauthorized access to, Confidential Customer Media that poses a threat to the security or confidentiality of the information.</p> <p>Secure Destruction Strategy: <i>The USPS® complies with this level of security control under its mail security policies in the Administrative Support Manual (ASM) Section 274.</i></p>
2.1e	<p>NAID Criteria: The Company has a written Incident Response Plan for responding to suspected or known security incidents. The Incident Response Plan must include a post-incident business impact analysis and a process for documenting all incidents and their outcomes.</p>

Item	NAID Criteria and USPS® Secure Destruction Strategy
	<p>Secure Destruction Strategy: <i>The USPS® complies with this level of security control under its mail security policies in the Administrative Support Manual (ASM) Section 274.</i></p>
2.2	<p>NAID Criteria: Access Individuals display Company-issued photo I.D. badges at all times while on duty. Badges must minimally include a photo, employee name and Company name.</p> <p>Secure Destruction Strategy: <i>All USPS® employees have badges. USPS® badge standards meet or exceed the NAID standard.</i></p>
2.11	<p>NAID Criteria: APPLIES TO PLANT-BASED AND/OR TRANSFER PROCESSING STATION CERTIFICATION ONLY. Unauthorized access to Confidential Customer Media in the designated secure destruction area and/or storage/staging areas is effectively prevented.</p> <p>Secure Destruction Strategy: <i>The USPS® does not use an outside vendor for Secure Destruction. All destruction is done within the USPS® by designated employees under security and legal controls equivalent to those for all classes of mail and far exceeding the legal sanctions established by NAID. Ongoing compliance is managed and monitored by the U.S. Inspection Service.</i></p>
2.12	<p>NAID Criteria: APPLIES TO PLANT-BASED AND/OR TRANSFER PROCESSING STATION CERTIFICATION ONLY All visitors entering the secure destruction building or Transfer Processing Station sign a log with their name, time in, affiliation, and time out. Visitors must be issued a Visitor Badge and be escorted or under the supervision of an Access Employee at all times while in the building. This log info/record must be maintained for one year.</p> <p>Secure Destruction Strategy: <i>The USPS® does not use an outside vendor for Secure Destruction. All destruction is done within the USPS®. USPS® visitor security standards exceed those of NAID. Inspection Service requires 1-year maintenance of visitor log controls. See eRIMS for details.</i></p>
3.1	<p>NAID Criteria: MEDIA ENDORSEMENT PAPER or PRINTED MEDIA is destroyed by commercial grade destruction equipment with the following OEM specifications or produces particle sizes no larger than those listed below (applicant to check and complete details for all equipment used):</p> <ol style="list-style-type: none"> 1. Continuous Shred: Width (max): 5/8 inch & Length: Indefinite 2. Cross Cut or Pierce & Tear: Width (max): 3/4 inch & Length (max): 2.5 inches 3. Pulverizer, Disintegrator or Hammermill* Screen Size (max): 2-inch diameter holes 4. Unspecified Equipment <p>Secure Destruction Strategy: <i>The USPS® utilizes centralized industrial cross cut destruction equipment for UAA RTS First-Class Mail® destined for secure destruction. The USPS® uses OEM shredding equipment with a specified maximum particle size not greater than ~1/4" by 1" (152mm²) Postal secure destruction particle size is much smaller than the allowable particle sizes defined by NAID.</i></p>

Item	NAID Criteria and USPS® Secure Destruction Strategy
3.6	<p>NAID Criteria: Destruction process has a method of quality control in place to ensure destroyed information is within the stated standards for the specific media endorsements for which the Company has applied.</p> <p><i>Secure Destruction Strategy: In coordination with the U.S. Inspection Service, the USPS® determines appropriate verification and inspection procedures that provide a quality control review of shredding performance.</i></p>
3.7	<p>NAID Criteria: Destroyed media must be disposed (sold, gifted, or discarded) in a responsible manner, which does NOT include any type of REUSE (for purposes such as animal bedding or packing materials). Applicant must attach a list of all current recipients (within past year) of destroyed media, indicating type of media and final disposition of materials by these recipients.</p> <p><i>Secure Destruction Strategy: The USPS® releases all shredded mail either to a recycling vendor or other vendor to ensure that agency recycling performance objectives are achieved. Reuse is not an option under this strategy. The USPS® maintains a list of the recycling contractors receiving this material. The USPS® updates its list of recycling contractors as they change.</i></p>

NAID criteria listed in the table below are not applicable to the Secure Destruction Program.

NAID Criteria not Applicable to Secure Destruction

Related to Employee Screening

- 1.2 (Part 3) Restrictive employee agreements in place that prevents drug screening and/or criminal record searches for certain individuals
- 1.3 Access Individuals, other than 1.2 exemptions, are monitored for drugs/substance abuse by one of the following methods:
 - On a random basis, 50% of employees are drug-screened annually
 - The local management has been trained in a qualified (pre-approved by NAID) “Substance Abuse Recognition Awareness Program”
- 1.4 All Access Employees have ongoing criminal record searches conducted in accordance with one of the following methods:
 - One-third of Access Individuals are randomly selected for criminal record searches annually
 - One-third of all Access Individuals are screened each year for three years (different individuals each year)
 - All Access Individuals have Criminal Record searches conducted every three years

Reason not Applicable to Secure Destruction:

- *Secure Destruction is not altering the underlying legislative and regulatory foundation of mail security standards governing the mail directed by Congress and these standards far exceed those of NAID in so far as they have the force of law and are subject to severe penalties under the United State Code (18 U.S.C 1905)*
- *No UAA RTS First-Class Mail® will leave a USPS® facility in a condition requiring security controls on securely destroyed information*

Related to Drivers Criteria

- 1.5 Drivers meet all licensing requirements of the governmental jurisdiction
- 2.1a Firm has written policies and procedures for drivers and destruction processing employees
- 2.1b Prior to gaining access to confidential material, all drivers and destruction processing employees must sign an acknowledgement indicating that they have received and read the Company’s current written policies and procedures each year
- 2.3 While at Customer’s location, drivers and other employees of contractor must wear a specific uniform

Reason not Applicable to Secure Destruction:

- *All Secure Destruction activities are performed by USPS® employees at secure USPS® facilities with 24/7 security systems*
- *No UAA RTS First-Class Mail® will leave a USPS® facility in a condition requiring security controls on securely destroyed information or drivers*

NAID Criteria not Applicable to Secure Destruction

Related to NAID Compliance

- 2.1f The Company has a written policy that addresses the procedures for employees to follow during an unannounced audit
- 2.1g All Access Employees must be trained annually to comply with the NAID AAA Certification requirements

Reason not Applicable to Secure Destruction:

- *USPS® is an independent establishment of the executive branch of the Federal Government with statutory authority to manage all mail within the United States from the moment it is deposited in a mail box to the time it is delivered to its intended customer*
- *The USPS® is governed by the Office of the Inspector General which has legislative authority to conduct audits²*
- *The US Postal Inspection Service conducts periodic reviews of mail security processes and procedures, including the USPS® SD Mail Service Program³*

Related to Media Destruction

- 2.4 At the time that media is transferred the Customer must be provided with a receipt or certificate of destruction indicating type and quantity of media and an acknowledgement of the services rendered. An electronic receipt is acceptable
- 2.5 All media for destruction are always attended by a Company employee or physically secured from unauthorized access while in the custody of the destruction contractor before they are destroyed
- 2.6 All media are securely contained during transfer from Customers' custody to transportation vehicle to prevent loss from wind or other atmospheric conditions
- 3.2 The ability to destroy Micro Media (Microfiche or Microfilm only) is certified based on commercial grade destruction equipment or process which produces a particle size of 1/8 inch maximum dimension or less
- 3.3 The Company has a written and verifiable process for the physical destruction (not wiping or overwriting) of conventional computer hard drives and prior to destruction event the Company provides Customers with a written description of the process for the physical destruction of computer hard drives, the serial numbers of all hard drives or CPUs destroyed are recorded, unless the Customer has signed an agreement opting out of this requirement, and the log of recorded serial numbers of hard drives destroyed is returned to the Customer upon the completion of the service, unless the Customer has opted out of this requirement
- 3.4 Non-Paper Media, as indicated below, are destroyed in accordance with the Company's standard method of destruction. Any method that deviates from this standard method of destruction must be communicated to the Customer in writing
- 3.5 *APPLIES TO PLANT-BASED CERTIFICATION ONLY* standard operating procedures for bin tips state that the destruction of confidential media must take place within 3 business days of arriving at the destruction facility, or the policies and procedures, the terms and conditions, or contracts used by the applicant must specify and reflect the actual time frame in which destruction is performed standard operating procedures for bin tips state that destruction occurs within an indicate timeframe for purges the destruction of confidential media must take place within 15 business days or the Customer must be notified

NAID Criteria not Applicable to Secure Destruction

Reason not Applicable to Secure Destruction:

- *Secure Destruction only applies to letter-sized UAA RTS First-Class Mail® not media or hard drive destruction*
- *USPS® does not transfer UAA RTS First-Class Mail® for destruction to other facilities once identified as such on the CIOSS equipment*
- *USPS® provides Secure Destruction a notification for each destroyed mailpiece – far exceeding NAID standards of bulk notifications*

Related to Vehicle

- 2.7 All vehicles used for transfer of media will have the applicable government inspection for roadworthiness on file
- 2.8 All vehicles used for transfer and/or destruction of media (whether intact or destroyed) will have lockable cabs and lockable, fully enclosed boxes. These vehicle cabs and boxes must be locked during transport and when unattended by Access Individual
- 2.9 All drivers of collection or destruction vehicles must have readily accessible two-way communication devices
- 2.10 Mobile Certification - The Company must perform mobile destruction services at the Customer's site

Reason not Applicable to Secure Destruction:

- *Secure Destruction only applies to letter-sized UAA RTS First-Class Mail® not media or hard drive destruction*
- *USPS® does not transfer UAA RTS First-Class Mail® for destruction to other facilities once identified as such on the CIOSS equipment*
- *No UAA RTS First-Class Mail® will leave a USPS® facility in a condition requiring security controls on securely destroyed information or drivers*

Applies to Plant-Based and/or Transfer Processing Station Certification Only

- 2.14 There is a monitored alarm system in place and utilized when the secure destruction building or Transfer Processing Station is unoccupied.
- 2.15 There is a closed circuit camera system monitoring all access points into the secure buildings/areas where confidential media are stored, processed and/or destroyed. All processing activities are monitored with sufficient clarity to identify people and their activities. There must be enough lighting at night or during other non-business hours to ensure that all images have sufficient clarity. NAID must be notified within 48 hours of the discovery of problems with the CCTV system which result in a loss of data, Recordings must be retained for 90 consecutive days in an organized, retrievable manner
- 2.16 Collection Facilities are used to store media as accepted by Customer and will be transferred to a destruction facility within 3 business days. Facility has restricted access with a monitored alarm system. The list of all Collection Facility locations associated with this plant-based operation is included with this Application
- 2.17 Transfer Processing Stations (TPS) are used to store materials for destruction no longer than 15 business days and meet the same operational requirements as a secure, plant-based destruction facility. The list of all TPS locations associated with this Branch is included with this Application. Each TPS will be charged an additional audit fee.
- 2.18 The following Operational Security systems are checked and maintained on a monthly basis:
 - Alarm System
 - Lighting

NAID Criteria not Applicable to Secure Destruction

- Door Locks
- Visitor Logs
- CCTV system (weekly basis, including a minimum of five minutes of playback)
- Monthly and Weekly Logs must be kept for one year

Reason not Applicable to Secure Destruction:

- All Secure Destruction activities are performed by USPS® employees at secure USPS® facilities with 24/7 security systems
- All destruction is done normally within the USPS® facility within 24 to 48 hours of UAA mail being identified for destruction

Related to Transfer of Custody (If Applicable)

- 3.8 Transfer of custody is used for each as indicated:
 - Temporary Staffing
 - Transportation (of media prior to destruction)
 - Other

Related to Customer Notification of Non-certified and/or Subcontracted Services

- 3.9 At the time of any information destruction bid or proposal, the Company must notify the potential customer in writing of the following scenarios, where applicable:
 - The information destruction service being proposed to the Customer is not NAID Certified at the time of the bid; and/or
 - The service will involve the use of one or more subcontractors, for either a portion of the destruction process (i.e. transportation, handling, or storage of material before destruction), or for the actual destruction of the media
 - In instances where a subcontractor will be used, this notification must identify the parties destined to accept custody, the exact location of destruction, and the method of destruction, if this information is known at the time of the bid or proposal. The notification must also indicate if a subcontractor performing destruction services is not NAID Certified

Reason not Applicable to Secure Destruction:

- All Secure Destruction activities are performed by USPS® employees at secure USPS® facilities with 24/7 security systems

Related to Company Assurances

- 4.1 Company is a legally registered business in the state of residence
- 4.2 General liability insurance (aggregate or umbrella) of \$2,000,000 or more

Reason not Applicable to Secure Destruction:

- USPS® is an independent establishment of the executive branch of the Federal Government with statutory authority to manage all mail within the United States from the moment it is deposited in a mail box to the time it is delivered to its intended customer
- The USPS® is an independent establishment of the executive branch of the Federal Government and is self-insured

International Standard for Destruction DIN 66399

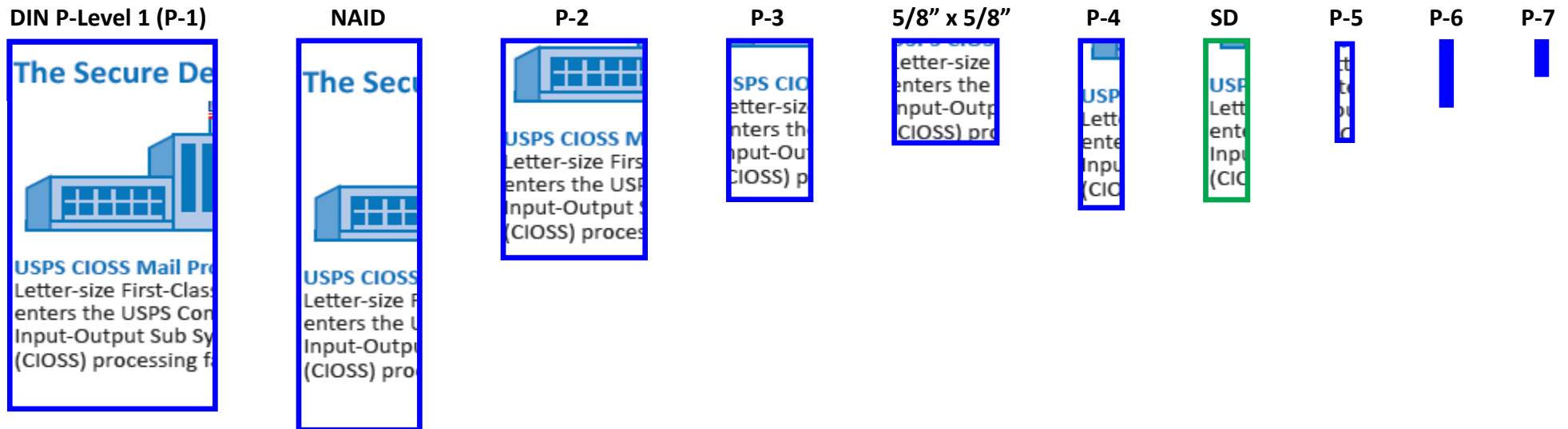
In addition to the NAID Criteria, Secure Destruction also meets and exceeds the International destruction level required for confidential information. DIN 66399 allows the following for paper destruction:

- **P-Level 1: General Data** surface area: ≤ to 2000mm² or strip width: ≤ 12mm (unlimited length)
- **P-Level 2: Internal Data** surface area: ≤ 800mm² or strip width: ≤ 6mm (unlimited length)
- **P-Level 3: Sensitive & Confidential Data** surface area: ≤ 320mm² or Strip width: ≤ 2mm (unlimited length)
- **P-Level 4: Particularly Sensitive & Confidential Data** surface area: ≤ 160mm² and strip width: ≤ 6mm
- **P-Level 5: Secret Data** surface area: ≤ 30mm² and strip width: ≤ 2mm
- **P-Level 6: Highly Secret Data** surface area: ≤ 10mm² and strip width: ≤ 1mm
- **P-Level 7: Top Secret Data** surface area: ≤ 5mm² and strip width: ≤ 1mm

USPS Secure Destruction Mail Service Option shreds/destroys the mail to P-Level 4 for both letter and flat mail.

Shred Size Reference

Below are actual shred sizes organized by largest surface area to smallest for NAID, DIN 66399 P-Levels, financial industry common practice of 5/8" x 5/8", and USPS Secure Destruction (SD).



¹ Mail sent back for destruction is considered live mail and part of the mail stream. Therefore, the mailers would be at no greater risk for liability than they are when they drop outgoing mail off for delivery. The Postal Service is a trusted institution that is enshrined in the U.S. Constitution. See U.S. Const. Art. 1, s. 8, cl. 7; 39 U.S.C. s. 101 (The Postal Service is “a basic and fundamental service provided to the people by the Government of the United States, authorized by the Constitution, created by Act of Congress, and supported by the people.”). Therefore, it is difficult to imagine a scenario under which a company would be found liable for entrusting the Postal Service to deliver mail to its final destination, whether that be a mailbox or a shredder located on-site at a USPS® facility. Further, the Federal Tort Claims Act (FTCA) includes a specific “postal matter” exception which excludes liability for any “claim arising out of the loss, miscarriage, or negligent transmission of letters or postal matter.” 28 U.S.C. 2680(b). This exception covers USPS® employee misappropriation of this information. See C.D. of NYC, Inc. v. U.S. Postal Service, 157 Fed. Appx. 428 (2d. Cir. 2005) (USPS® not liable for mail stolen by USPS® employees).” *Carrie M. Branson, Chief Counsel, Tort, USPS® Law Department.*

² It is important to note that the Federal Information Security Management Act of 2002 does not apply to the U.S. Postal Service. We comply with it voluntarily as a general rule. However, we are not included in the definition of “agency” in the law. The details: FISMA defines “agency” by cross-reference to the definition of “agency” in the Paperwork Reduction Act (44 USC 3502). See 44 USC 3452(a). Courts have consistently found that the Postal Service is not an “agency” under the Paperwork Reduction Act definition. See *Kuzma v. USPS®*, 798 F.2d 29 (2nd Cir. 1986); *Shane v. Buck*, 658 F.Supp. 908 (D. Utah 1985), *aff’d* 817 F.2d 87 (10th Cir. 1987). The law clearly falls within the scope of 39 USC 410(a), which exempts the Postal Service from laws generally regulating the operation of Federal agencies.

³ In addition to the work performed by Postal Inspectors to protect security of the mail, the USPS® Office of Inspector General (OIG) will investigate any allegations of mail theft by individuals and entities under contract with the Postal Service to facilitate the *Secure Destruction* process per Title 18, United States Code. Postal Inspection Service has agreed to conduct periodic security assessments of the Secure Destruction processes and procedures in place at USPS® facilities.

* Based on the NAID 2014 Standard.