SECURITY PROFILE FOR THIRD PARTY DATA ACCESS

Prepared for:

The NIST SGIP Cyber Security Working Group

&

The UCAIug SG Security Working Group

Prepared by:

The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG)

Managed by:

EnerNex Corporation
620 Mabry Hood Road
Knoxville, TN 37923
USA
(865) 218-4600
www.enernex.com

Version
0.20

Revision History

Rev	Date	Summary	Marked
0.07	12/15/09	Incorporated use case descriptions.	N
0.08	12/16/09	More use case changes; including insertion of Use Case 3a.	N
0.12	1/14/10	Significant overhaul of Sections 1, 3, and 4.3. Re-organization of Section 4.	N
0.13	1/18/10	Developed Section 4.3. Various edits throughout Sections 3 and 4.	N
0.14	1/19/10	Unified language in preconditions and guarantees in use cases; renumbered use cases; also added explanation of use case template.	N
0.15	1/19/10	Revised/edited Section 3 and Section 5 introduction.	N
0.16	1/26/10	Incorporated material from separate documents for Sections 5 and 6.	N
0.17	1/28/10	Editing pass.	N
0.18	1/28/10	Combined comments from ASAP-SG team	Y
0.19	1/29/10	Editing pass – resolved changes from ASAP-SG team review. Added Executive Summary and Appendix C (References).	N
0.20	1/29/10	Cleanup of final internal ASAP-SG comments.	N

Executive Summary

This document delineates the security requirements for individuals, utilities, and vendors participating in a three-way relationship that involves the ownership and handling of sensitive data. Specifically this document is aimed at the smart grid environment, and is intended to address the concerns of electric utility customers who want to allow value added service providers to access electric usage data that is in the custody of the customer's utility. Other three-way data sharing scenarios may also be addressed using this profile, as the roles of the three parties have been abstracted in such a way as to support mapping to different environments.

This document defines a set of security-centric use cases and adapts controls from the Department of Homeland Security Catalog of Control Systems Security (U.S. Department of Homeland Security, 2009). The overall approach is to delineate an overarching pattern through the use cases and subsequently link the three parties to individual security control recommendations on a use case (and sometimes use case step) basis. The use cases are explicitly designed to be modular in nature so as to facilitate combining them in different arrangements to describe differing business models.

The primary audience of this document is organizations that are developing or implementing solutions requiring or providing access to energy-related data owned by one entity but held by a different entity. This document is written at the normal level of utility security experience for system owners, system implementers and security engineers.

Table of Contents

Table of Figures

Acknowledgements

The Advanced Security Acceleration Project for Smart Grid (ASAP-SG) would like to thank:

- Supporting utilities, including American Electric Power, BC Hydro, Con Edison Consumers Energy, Florida Power & Light, Oncor, and Southern California Edison.

- Supporting organizations including The United States Department of Energy and the Electric Power Research Institute.

- The members of the UCAIug OpenSG OpenADE Task Force and participants in NIST PAP10 activities that provided ASAP-SG with essential foundational knowledge and insight into the Third Party Data Access problem space.

ASAP-SG would also like to thank the Department of Homeland Security (DHS) Cyber Security Division, National Institute of Standards and Technology (NIST) Computer Security Division, and North American Reliability Corporation (NERC) for the works that they have produced that served as reference material for the Third Party Data Access Security Profile.

The ASAP-SG Architecture Team included resources from Consumers Energy, EnerNex Corporation, InGuardians, Oak Ridge National Laboratory, the Software Engineering Institute at Carnegie Mellon University, and Southern California Edison.

Authors

Len Bass

Bobby Brown

Kevin Brown

Matthew Carpenter

Pat Donohoe

James Ivers

Teja Kuruganti

Howard Lipson

Jim Nutaro

Justin Searle

Brian Smith

James Stevens

Edited by: Darren Highfill

1 Introduction

This document presents the security profile for third party data access. In this context, we assume a third party to be any entity that requests access to data in the custody of someone besides the owner. We refer to the relevant entities herein as a Resource Owner, a Resource Custodian, and a Third Party.

By way of example, a Resource Owner could be an electric utility customer and their utility could fill the role of a Resource Custodian by managing the customer's electricity usage data. A Third Party could enter the picture by providing the customer (Resource Owner) a value added service (e.g., data analysis) that requires access to data in the custody of the customer's utility (Resource Custodian).

For the purposes of this document, we assume the Resource Owner to be the rightful owner of a specific set of data in the custody of the Resource Custodian. The addition of a Third Party into this custodial relationship creates a complex and volatile trust environment. Systems must be purposefully engineered to accommodate many types of asynchronous changes in varying order without compromising stakeholder interests.

It is with this goal in mind that we put forth a basic set of modular use cases that may be combined to portray complete real-world business sequences, and associate security controls with each sequence and its participants. This approach provides an unambiguous means for any entity involved in third party data access to determine precisely which security controls are required of them based on the activities in which they participate. Regardless, the value added services offered by Third Parties will evolve over time, and therefore the scope and extent of this security profile must evolve with them.

1.1 Scope

The current scope of this security profile is the mechanisms by which a Resource Owner (such as a residential utility customer) grants permission for a Resource Custodian (such as a utility) to share its data (such as meter usage data) with a Third Party so that the Third Party may provide a desired service (such as energy consumption analysis) to the Resource Owner. These roles are elaborated in Section 2.1. The specific use cases defining this relationship are described in Section 2.4.[1]

A fundamental scoping decision is that a Resource Owner's data maintained by the Resource Custodian is in scope, as is the actual delivery of that data to the Third Party. Data after it has been delivered to the Third Party is out of scope; however we do recommend certain attestations on behalf of the Third Party relevant to their handling of the data. A fundamental concern of this security profile is not to share any of the Resource Owner's sensitive information such as Personally Identifiable Information (PII) between the Resource Custodian and the Third Party. [2] Any PII the Resource Owner may have independently shared with the Third Party is out of scope for this version of the security profile.

This version of the security profile does not address data that a Third Party may want to share with a Resource Owner (such as demand response signals to be sent to a customer's premises). Such data may be covered in a future version of this profile.

1.2 Third Party Data Access Pattern

This security profile is focused on the establishment, operation, and termination of a relationship among three parties—a Resource Owner, a Resource Custodian, and a Third Party. In this relationship, a Third Party wants to provide some service to a Resource Owner, but requires resource data owned by the Resource Owner to provide the service. The Resource Custodian maintains the required information and is granted permission by the Resource Owner to share this information with the Third Party. Figure 1 depicts this relationship as a pattern among these three roles.

---

[1] These use cases are based in part on the use cases described in the OpenADE Business and User Requirements Document.

[2] PII includes name, address, or other information that can be uniquely associated with an individual's "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." as defined by GAO Report 08-343, Protecting Personally Identifiable Information (http://www.gao.gov/new.items/d08343.pdf) (United States Government Accountability Office, 2008) and NIST SP800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (Draft) (http://csrc.nist.gov/publications/drafts/800-122/Draft-SP800-122.pdf) (National Institute of Standards and Technology, 2009). This principle may also be applied to other customer entities (e.g. a business) with a different set of parameters.

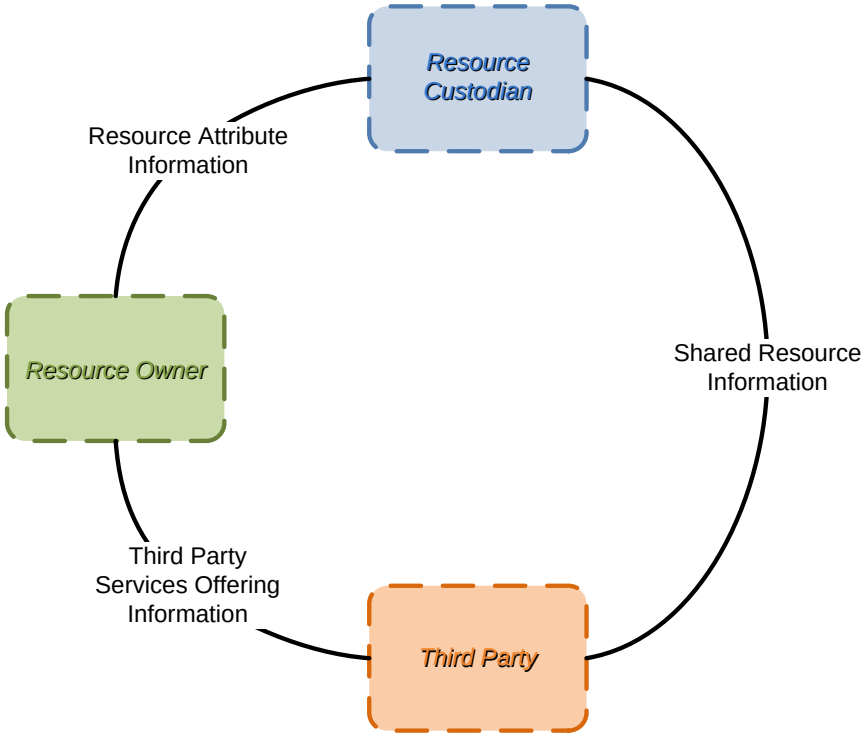

Figure 1: The Third-Party Data Access Pattern

1.2.1 Interactions

In this relationship

- Resource Owners interact with Resource Custodians to select the resource (e.g., usage data for a particular meter) for which they wish to grant access to a Third Party and any necessary attributes of the relationship (e.g., the period during which a Third Party should have access).
- Resource Owners interact with Third Parties to establish a service relationship. The bulk of this relationship (e.g., any business or contractual details) is out of scope for this profile. How a Resource Owner establishes the link between the Third Party and a Resource Custodian, however, is in scope.
- Resource Custodians provide Third Parties with shared resource information (e.g., usage data) in accordance with the permission granted by the Resource Owner.

The approach taken in this profile is to present several use cases depicting the interactions among the roles participating in this pattern.

1.2.2 Relationship

A third-party data access relationship is defined by a particular resource and the relevant three parties (Resource Owner, Resource Custodian, and Third Party). Each combination thereof constitutes a unique third-party data access relationship.

It is important to note that some Resource Owners may have more than one resource they wish to share (e.g., data for more than one electric service point). In such cases, each resource is the subject of a separate third-party data access relationship, even if the relationship has the same Resource Owner, Resource Custodian, and Third Party. In other cases, a Resource Owner may choose to share the same resource with multiple Third Parties, also resulting in a separate third-party data access relationship for each Resource Owner, Resource Custodian, and Third Party combination even if the relationship refers to the same resource.

1.3 Approach

The overall approach is to delineate the pattern through use cases and subsequently link the roles and sometimes the use case steps to security control recommendations. Much of the foundational work herein (notably including the use cases) was created based on extensive discussions with members of the OpenADE Task Force within the UCAIug. While some use case material existed, we did not find sufficient modularity from a strict security perspective to describe the myriad ways in which third party data access might be accomplished. Instead, our goal for this document is to provide guidance for a broad and intentionally open-ended set of potential solutions.

Accordingly we developed our own use cases that utilized available reference material as a starting point, yet abstracted the scenarios to a level that allows for selection from a wide variety of solution designs. These use cases are an essential component of the security analysis herein.

These use cases are explicitly designed to be modular in nature – that is, to facilitate combining them in different arrangements to describe differing business models. We describe both “push” and “pull” models, and endeavor to allow for as broad a structure as possible given the emergent nature of the marketplace. While this version of the security profile does not address demand-response, later versions may indeed describe recommendations for control signals between the Third Party and the Resource Owner – either directly or through the Resource Custodian.

The use cases are also designed with an intentional level of abstract reference to security functionality and include no security controls in the step descriptions, relegating all security controls to their own section of the document. Selection of controls generally follows the approach described in the Smart Grid Security Profile Blueprint (ASAP-SG, 2009). This document references the DHS Catalog of Control Systems Security: Recommendations for Standards Developers (U.S. Department of Homeland Security, 2009) and tailors the controls them for third party data access.

All recommended controls have at least been modified by removing the word “control” from the “control systems” reference; as we do not feel third party data access scenarios comprise a control system under the current set of use cases. Some of the controls have been modified further to reflect considerations of specific use cases or even use case steps; and in rare cases we have developed our own controls where no existing DHS control was a close enough fit to adequately address concerns.

1.4 Audience

The primary audience of this document is organizations that are developing or implementing solutions requiring or providing access to energy-related data owned by one entity but held by a different entity. This document is written at the normal level of utility security experience for system owners, system implementers and security engineers. The user is assumed to be experienced at information asset risk estimation. The user is further assumed to be knowledgeable in developing security requirements and guidance.

1.5 Disclaimer/Status

Please note that the recommended controls listed in this document are adaptations of the DHS controls as appropriate for third party data access security. The DHS control section numbers are only provided for traceability, and not intended to indicate that the controls in this document are the DHS controls themselves. Where the ASAP-SG team has created controls for which there was no DHS counterpart, the "ASAP-" prefix is used instead of "DHS-".

2 Analysis

This section elaborates on the roles involved in the third-party data access pattern described in Section 1.2, the mapping of these abstract roles to several concrete applications, the high-level security constraints on successful application of the pattern, and the use cases that may be implemented in realizing this relationship.

2.1 Roles

The relationship among these roles can be realized in different settings (as shown in Section 2.2) among different actors. This section describes the characteristics of each abstract role, solely as it pertains to this relationship.

2.1.1 Resource Owner

A Resource Owner produces and owns the resource information managed by a Resource Custodian. A typical Resource Owner would be an electric utility customer and a typical example of resource information owned by the customer is their electricity usage data.

2.1.2 Resource Custodian

A Resource Custodian manages resource information on behalf of a Resource Owner and will share this information with Third Parties only in accordance with the wishes of the Resource Owner. A Resource Custodian typically has direct access to the pertinent information (e.g., by directly acquiring electricity usage data from a meter).

2.1.3 Third Party

A Third Party provides some service to a Resource Owner based on information it does not have direct access to; instead, a Third Party relies on a Resource Custodian to provide it with a Resource Owner's information. This relationship requires a set of agreements between Resource Owner-Third Party, Resource Owner-Resource Custodian, and Third Party-Resource Custodian to ensure that the appropriate information is provided as needed and only that information is shared.

While a Third Party may have access to some personally identifiable information about a Resource Owner, it will only have information that has been directly supplied by the Resource Owner. A Resource Custodian will not provide a Third Party with a Resource Owner's personally identifiable information.

2.2 Mapping to Concrete Applications

The pattern for the third-party data access relationship shown in Figure 1 and the use cases governing this relationship described in Section 2.4 can be applied to different sets of actors realizing this pattern. In this section, we demonstrate several such possible applications of the pattern.

2.2.1 Application of Pattern – Vertically Integrated Utility

Figure 2 shows how this pattern could be applied in a setting in which a vertically integrated utility fills the role of the Resource Custodian and a value-added service provider (VASP) fills the role of the Third Party.

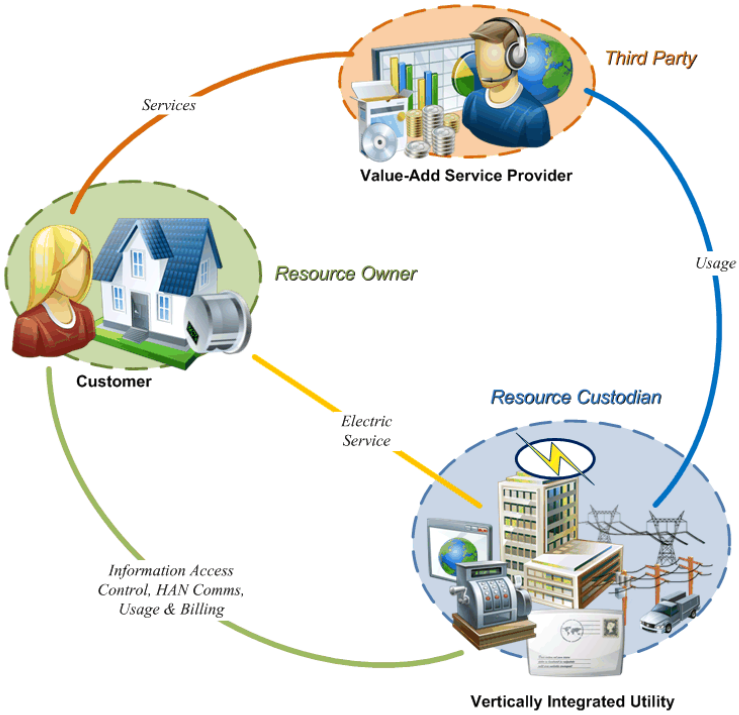

Figure 2: Application of Pattern - Vertically Integrated Utility

The Resource Owner is a residential electric utility customer and the resource to be shared is the customer's electricity usage data.

The Resource Custodian is a vertically integrated electric utility. The utility provides the customer with electric service and has direct access to the customer's electricity usage data (e.g., through remote meter reads via an AMI system) and is willing to share this data with Third Parties at the customer's request. The utility provides some means for the customer to manage third-party data access relationships, such as through a web-based customer portal. The utility also has other interactions with the customer, such as billing functions and interaction with devices in the customers home area network (HAN), but these interactions are not governed by this profile.

The Third Party is a value-added service provider offering some service to the customer (e.g., assistance in monitoring and managing electricity usage). The customer establishes a business relationship with the VASP for these services (the terms and management of which are not governed by this profile) and the VASP provides some means for the customer to manage the service (e.g., through a web-based portal). The VASP needs access to the customer's electricity usage data in order to provide its service. The customer establishes the third-party data access relationship with the VASP and the utility, enabling the VASP to access the customer's electricity usage data from the utility.

The interactions between the customer and the utility to manage the third-party data access relationship, between the customer and the VASP to manage the relationship, and the VASP and the utility to access the customer's electricity usage data are all described

in Section 2.4 and the security controls needed by systems implementing these interactions are described in Section 3.

2.2.2 *Application of Pattern – Independent Portal*

Figure 3 shows how this pattern could be applied in a setting in which an independent customer portal (e.g., not run by a vertically-integrated utility) fills the role of the Resource Custodian and a value-added service VASP fills the role of the Third Party. This application could be combined with the example in Section 2.2.3 (e.g., as might be seen in Texas).

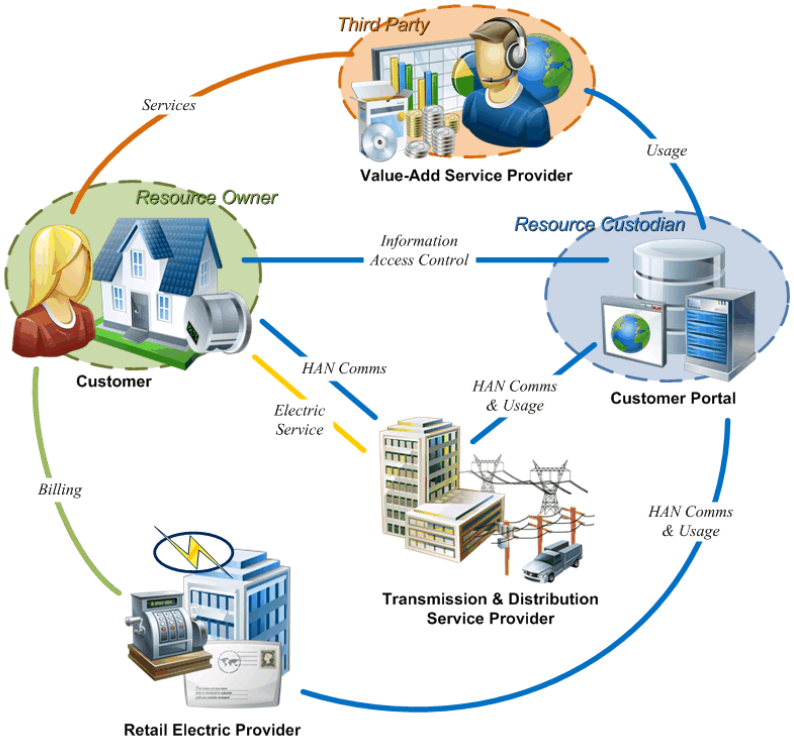

Figure 3: Application of Pattern - Independent Portal

This application of the pattern is very similar to that described in Section 2.2.1. As in that example, the Resource Owner is a residential electric utility customer, the resource to be shared is the customer's electricity usage data, and the Third Party is a value-added service provider offering some service to the customer.

This example differs in that there is no single, vertically-integrated utility. Instead, utility functions are distributed among three actors. The transmission and distribution service provider (TDSP) provides electric service to the customer and handles any HAN communications. A separate retail electric provider (REP) manages the entirety of the

customer relationship from a utility standpoint, including billing functions. Neither of these actors takes part in the third-party data access relationship with the Third Party.[3]

The Resource Custodian is a customer portal operated by an independent entity (i.e., neither the REP nor the TDSP). For example, in Texas such a portal is collectively run by the TDSPs. The customer portal has access to the customer's electricity usage data (e.g., through interactions with the transmission and distribution utility not specified herein) and is willing to share this data with Third Parties at the customer's request. The customer portal provides some means for the customer to manage third-party data access relationships.

2.2.3 *Application of Pattern: Retail Electric Provider*

Figure 4 shows how this pattern could be applied in a setting in which an independent customer portal (e.g., not run by a vertically-integrated utility) fills the role of the Resource Custodian and a retail electric provider fills the role of the Third Party. This application could be combined with the example in Section 2.2.2 (e.g., as might be seen in Texas).

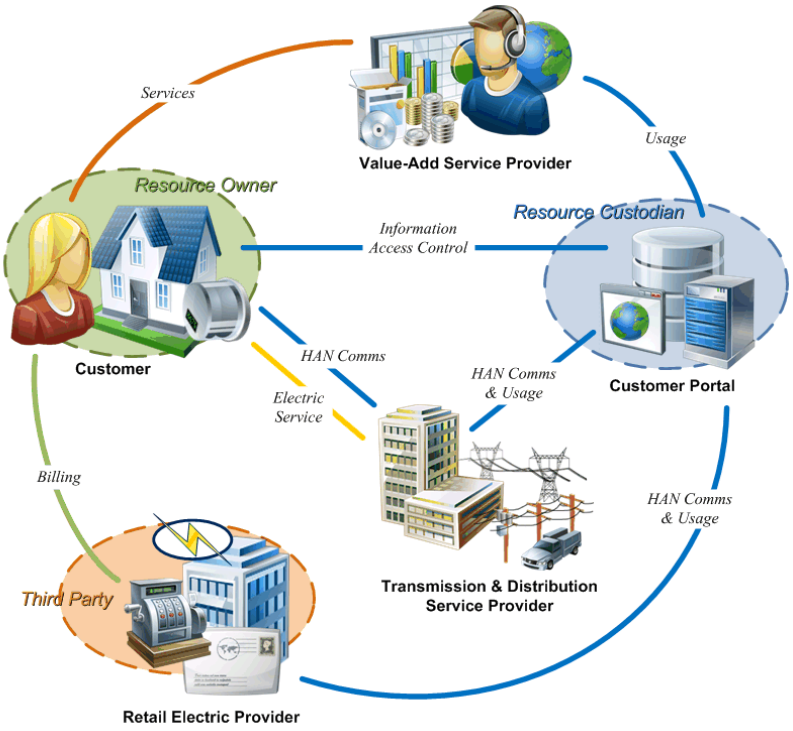

Figure 4: Application of Pattern - Retail Electric Provider

[3] This version of the Security Profile for Third Party Data Access only deals with the sharing of data from a Resource Custodian to a Third Party. Future versions of this profile may expand this scope by, for example, including communications from a Third Party to a HAN device owned by a Resource Owner.

This application of the pattern is very similar to that described in Section 2.2.2. As in that example, the Resource Owner is a residential electric utility customer, the resource to be shared is the customer's electricity usage data, and the Resource Custodian is an independent customer portal.

In this application, the Third Party is a retail electric provider. The REP, in order to perform billing functions, needs access to the customer's electricity usage data. The REP gets this data from the customer portal using the third-party data access profile.

In Texas, a common customer portal is run by the transmission and distribution service providers. Customers can use this portal to choose a REP and set up a third-party data access relationship. In that situation, choosing a REP maps to the first use case (Section 2.4.1), giving the customer portal permission to share the customer's electricity usage data with the REP. Likewise, a customer "shopping around" for a REP may grant each prospective REP temporary access to electricity usage data for the purposes of determining a proposed rate.

Note that multiple applications of the pattern can appear in a single setting. For example, in Texas 2.2.2 and 2.2.3 are both used. A customer participates in two third-party data access relationships—one with a value-added service provider and one with a retail electric provider. These relationships are treated separately herein as there is no interaction between the Third Parties that is in scope for this profile.[4]

2.3 Security-related Constraints

The security issues for third-party data access are all rooted in concern over the handling of an asset (Resource) which is assumed to be electricity usage data in the majority of the cases herein. The specific cause for concern is that the owner (Resource Owner) of the asset is not in direct control of the asset. The entities handling the asset (Resource Custodian and Third Party) must therefore protect the interests of the owner. Accordingly, this profile is focused on delineating a common baseline understanding of reasonable and fair expected behavior for each of the primary roles (Section 2.1) in this pattern.

As a starting point, it is assumed that the Resource Owner wants certain pieces of their information to be shared with parties they select. Conversely, it is assumed that the Resource Owner does not necessarily want all of their information shared, nor do they want even certain pieces to be shared with parties they have not selected.

The following “ground rules” (security-related constraints) guided the development of the use cases found in Section 2.4 and the determination of recommended controls found in Section 3:

[4] Relationships involving multiple third parties are modeled by splitting them into multiple relationships and examining them individually. Direct relationships between third parties are not the concern of this security profile.

1. A Resource Custodian shall not release PII to a Third Party.
2. A Resource Custodian shall not disclose any sensitive Resource Owner data[5] without explicit authorization by the Resource Owner.
3. A Third Party shall not disclose any sensitive Resource Owner data without explicit authorization by the Resource Owner.
4. A Resource Owner requesting/granting access to Resource Data must be authenticated and authorized to manage privileges for that data.
5. A Resource Owner shall always receive timely notification of changes in access to their sensitive data.
6. Only trusted Third Parties shall participate in the exchange of data.
7. Resource Data must be exchanged in a secure fashion. (Note: This document neither assumes nor dictates communication technology parameters regarding the exchange.)
8. A Resource Owner may use a simple interface (e.g., a web browser) to interact with Resource Custodians and Third Parties. (Resource Custodians and Third Parties shall not place undue technological sophistication expectations on the Resource Owner.)

While the use cases were written without inclusion of specific security controls, these constraints are reflected in the contained steps, such as through explicit inclusion of notifications or use of a Shared Resource Key to avoid disclosure of PII. These constraints also provided significant input into the determination of appropriate security controls, as documented throughout Section 3.

2.4 Use Cases

This section presents a superset of the use cases that are needed to realize the third-party data access relationship. Alternative use cases are presented for activities that can be achieved in different ways, such as the delivery of shared resource information by push or by pull.

This security profile includes the following use cases:

Use Case 1: Resource Owner Establishes Relationship via Resource Custodian

Use Case 2: Resource Owner Establishes Relationship via Third Party

Use Case 3: Resource Owner Modifies Permissions

Use Case 4: Resource Owner Terminates Relationship

[5] Sensitive data will be defined by the Resource Owner, Resources, Custodian and Third Party during service or contract discussions.

Use Case 5: Resource Custodian Terminates Relationship

Use Case 6: Third Party Terminates Relationship

Use Case 7: Third Party Establishes Subscription with Resource Custodian

Use Case 8: Resource Custodian Notifies Third Party of Resource Availability

Use Case 9: Resource Custodian Sends (Pushes) Resource to Third Party

Use Case 10: Third Party Receives (Pulls) Resource from Resource Custodian

Use Cases 1-6 collect functions needed to establish, maintain, and terminate the third party data access relationship for a particular resource that is owned by a Resource Owner and controlled by a Resource Custodian:

- Use Cases 1 and 2 present alternative means for a Resource Owner to establish the relationship, varying in terms of which role is used to initiate the relationship;
- Use Cases 3 and 4 present the means for the Resource Owner to modify and terminate the relationship.
- Use Cases 5 and 6 present the means by which the other roles, Resource Custodian and Third Party, can terminate the relationship.

Use Cases 7-10 collect functions needed to carry out third party data access via an established relationship for a particular resource.

- Use Case 7 presents the means for the Third Party to establish a subscription indicating its interest in receiving resource data from a Resource Custodian.
- Use Cases 8-10 represent two alternatives for data sharing—a push model and a pull model.
    - The push model is presented in Use Case 9, in which the Resource Custodian sends the resource data to the Third Party.
    - The pull model is presented in Use Cases 8 and 10; in this model, the Resource Custodian sends notification of data availability to the Third Party, but waits for a request (the pull) before sending the resource data.

These use cases do *not* include security controls, such as the use of authentication or encryption. Security controls and their mapping to these use cases are found in Sections 4 and 3 respectively.

The concept of a Shared Resource Key is used throughout these use cases. A Shared Resource Key is a token used to uniquely identify an instance of a third-party data access relationship (i.e., each Resource Owner-Resource Custodian-Third Party combination for a particular resource will have a unique Shared Resource Key). A Shared Resource Key contains no PII regarding the Resource Owner and so can be freely shared among all three roles without unnecessary disclosure of sensitive information. Once the relationship is established, inclusion of a Shared Resource Key in an interaction is sufficient to identify a specific third-party data access relationship.

Each use case contains the following sections

- Use Case Description: This is a summary of the use case, describing the overall flow and steps.
- Preconditions: These are conditions that must be true for the use case to be successfully executed.
- Minimal Guarantees: These are properties that will be true any time the use case is initiated, regardless of whether it terminates successfully.
- Success Guarantees: These are properties that will be true only if the use case terminates successfully. This requires that all preconditions and all condition checks (e.g., for validity of a request) be satisfied during execution of the use case.
- Trigger: This is the stimulus that initiates execution of the use case.
- Main Success Scenario: This defines the series of steps undertaken by each role during successful execution of the use case. The scenario is depicted graphically in a Unified Modeling Language (UML) activity diagram and each step is summarized in text.

2.4.1 Use Case 1: Resource Owner Establishes Relationship via Resource Custodian

Use Case Description: An owner of a particular resource (Resource Owner) wants to grant permission for a Resource Custodian to share that resource with a Third Party. The Resource Owner initiates the process through the Resource Custodian.

Preconditions:

- Resource Owner has established accounts with Resource Custodian and Third Party.
- Third Party has an established account with Resource Custodian.

Minimal Guarantees:

No resource data or personal data is provided to the Third Party by the Resource Custodian as part of this interaction.

Success Guarantees:

- A Shared Resource Key is generated to allow all three roles to refer to the same shared resource without disclosing personally identifiable information. This key is known to all three roles.
- The Third Party has the Resource Owner's permission to get the specified resource data from the Resource Custodian.

- The Resource Custodian sends the Resource Owner confirmation of establishment of the third-party data access relationship.

Trigger:

The Resource Owner decides to grant permission for the Resource Custodian to share their resource data with the Third Party.

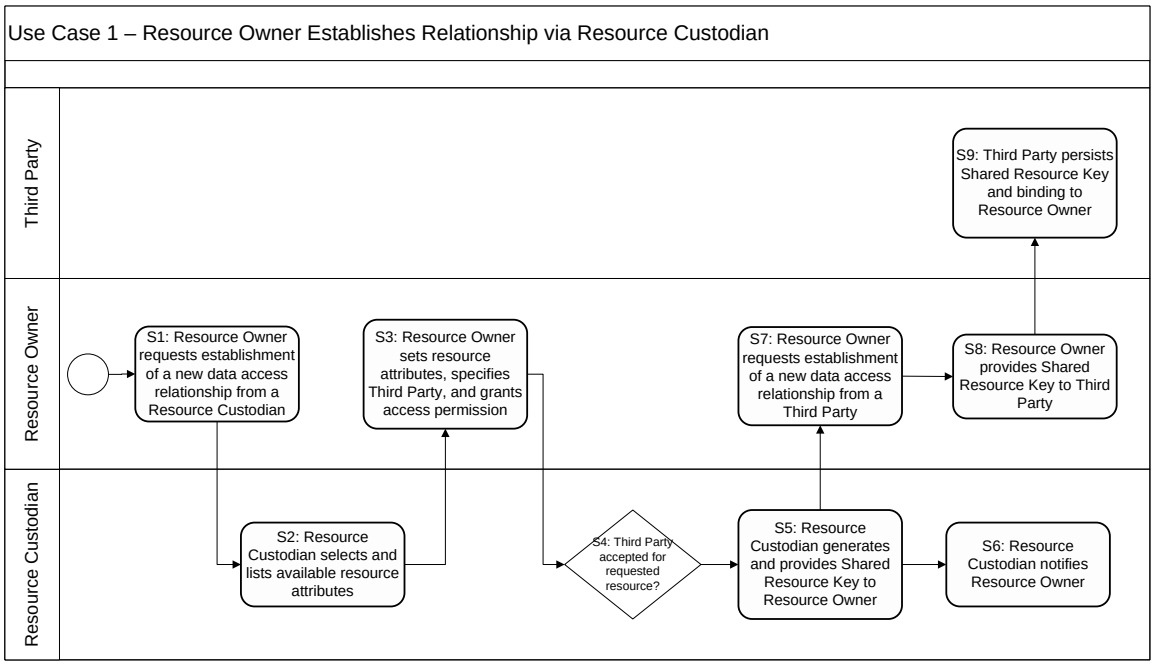

Diagram: Use Case 1

Main Success Scenario:

S1: Resource Owner requests that the Resource Custodian establish a new data access relationship.

S2: Resource Custodian presents the Resource Owner with a list of resources that can be shared with Third Parties. Any additional attributes (e.g., duration for which permission should be granted) that can be selected are also presented.

S3: Resource Owner selects a resource to share, sets any available attributes for the relationship, and specifies a Third Party that is known to the Resource Custodian. Selecting these parameters and completing the interaction indicates permission for the Resource Custodian to grant the specified Third Party access to the specified shared resource.

S4: The relationship will only be created if the Resource Custodian accepts the selections for the Third Party (e.g., a Resource Custodian may constrain access to certain resource attributes depending on resource sensitivity).

S5: Resource Custodian generates a Shared Resource Key for this relationship and provides it to the Resource Owner. Each Shared Resource Key is unique to the

relationship between a Resource Owner, Resource Custodian, and Third Party for a particular resource.

S6: Resource Custodian notifies Resource Owner of the creation of the Shared Resource Key and establishment of the relationship. No acknowledgment or confirmation is required.

S7: Resource Owner requests that the Third Party complete the establishment of the new data access relationship.

S8: Resource Owner provides the Shared Resource Key to the Third Party.

S9: Third Party persists the Shared Resource Key, associating it with its relationship with the Resource Owner.

2.4.2 Use Case 2: Resource Owner Establishes Relationship via Third Party

Use Case Description: An owner of a particular resource (Resource Owner) wants to grant permission for the Resource Custodian to share that resource with a Third Party. The Resource Owner initiates the process through the Third Party.

Preconditions:

- Resource Owner has established accounts with Resource Custodian and Third Party.
- Third Party has an established account with Resource Custodian.

Minimal Guarantees:

No resource data or personal data is provided to the Third Party by the Resource Custodian as part of this interaction.

Success Guarantees:

- A Shared Resource Key is generated to allow all three roles to refer to the same shared resource without disclosing personally identifiable information. This key is known to all three roles.
- The Third Party has the Resource Owner's permission to get the specified resource data from the Resource Custodian.
- The Resource Custodian sends the Resource Owner confirmation of establishment of the third-party data access relationship.

Trigger:

The Resource Owner decides to grant permission for the Resource Custodian to share a specific resource with the Third Party.

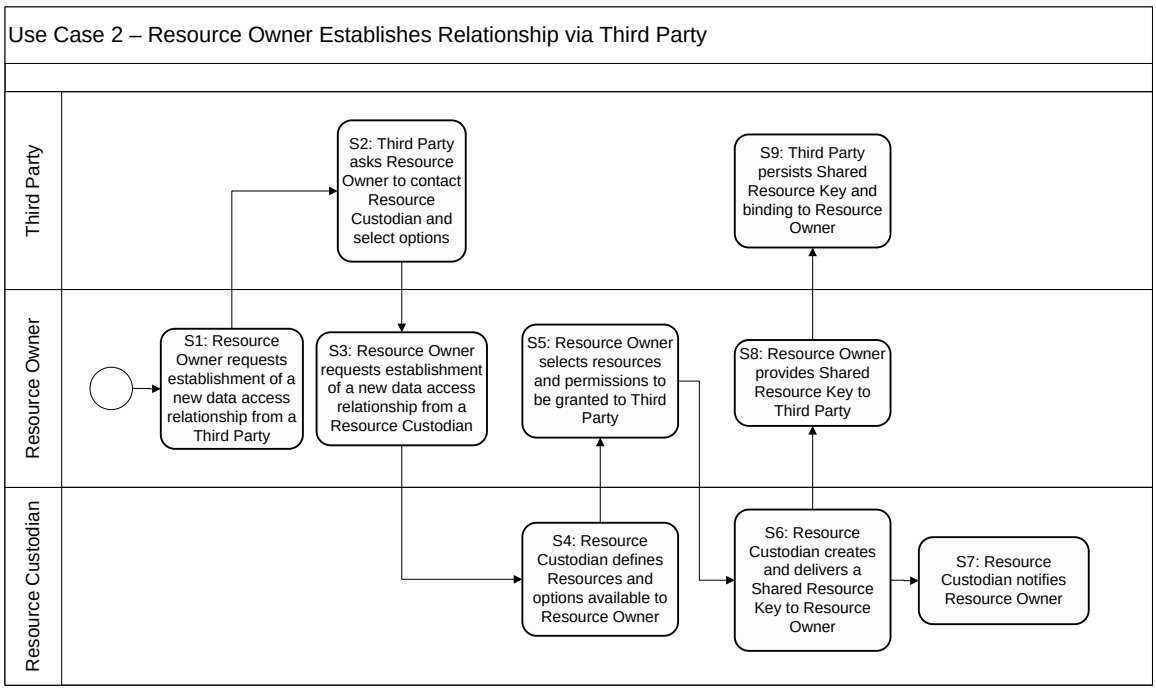

Diagram: Use Case 2

Main Success Scenario:

S1: Resource Owner requests that the Third Party establish a new data access relationship.

S2: Third Party directs Resource Owner to appropriate Resource Custodian (perhaps via selection from a list of Resource Custodians with which the Third Party has established a relationship) to select options for the data access relationship. Selections will be made directly with the Resource Custodian.

S3: Resource Owner requests that the Resource Custodian establish a new data access relationship.

S4: Resource Custodian presents the Resource Owner with a list of resources that can be shared with Third Parties. Any additional attributes (e.g., duration for which permission should be granted) that can be selected are also presented.

S5: Resource Owner selects a resource to share, sets any available attributes for the relationship, and specifies a Third Party that is known to the Resource Custodian. Selecting these parameters and completing the interaction indicates permission for the Resource Custodian to grant the specified Third Party access to the specified shared resource.

S6: Resource Custodian generates a Shared Resource Key for this relationship and provides it to the Resource Owner. Each Shared Resource Key is unique to the relationship between a Resource Owner, Resource Custodian, and Third Party with respect to a particular resource.

S7: Resource Custodian notifies Resource Owner of the creation of the Shared Resource Key and establishment of the relationship. No acknowledgment or confirmation is required.

S8: Resource Owner provides the Shared Resource Key to the Third Party.

S9: Third Party persists the Shared Resource Key, associating it with its relationship with the Resource Owner.

2.4.3 Use Case 3: Resource Owner Modifies Permissions

Use Case Description: The Resource Owner has an existing third party data access relationship with a particular Resource Custodian and Third Party and wants to either extend or restrict the permissions associated with that relationship.

Preconditions:

- Third Party has an established account with Resource Custodian.
- Resource Owner has established a third-party data access relationship with the Resource Custodian and the Third Party with respect to a particular resource, resulting in a unique Shared Resource Key identifying the relationship.

Minimal Guarantees:

No resource data or personal data is provided to the Third Party by the Resource Custodian as part of this interaction.

Success Guarantees:

- Future interactions between the Resource Custodian and the Third Party with respect to the specified resource are governed by the modified permissions.
- The Third Party deletes any data not allowed by the new permissions for the relationship.
- The Resource Custodian sends the Resource Owner confirmation of modification of the permissions of the third-party data access relationship.

Trigger:

Resource Owner decides to modify the conditions governing a third-party data access relationship.

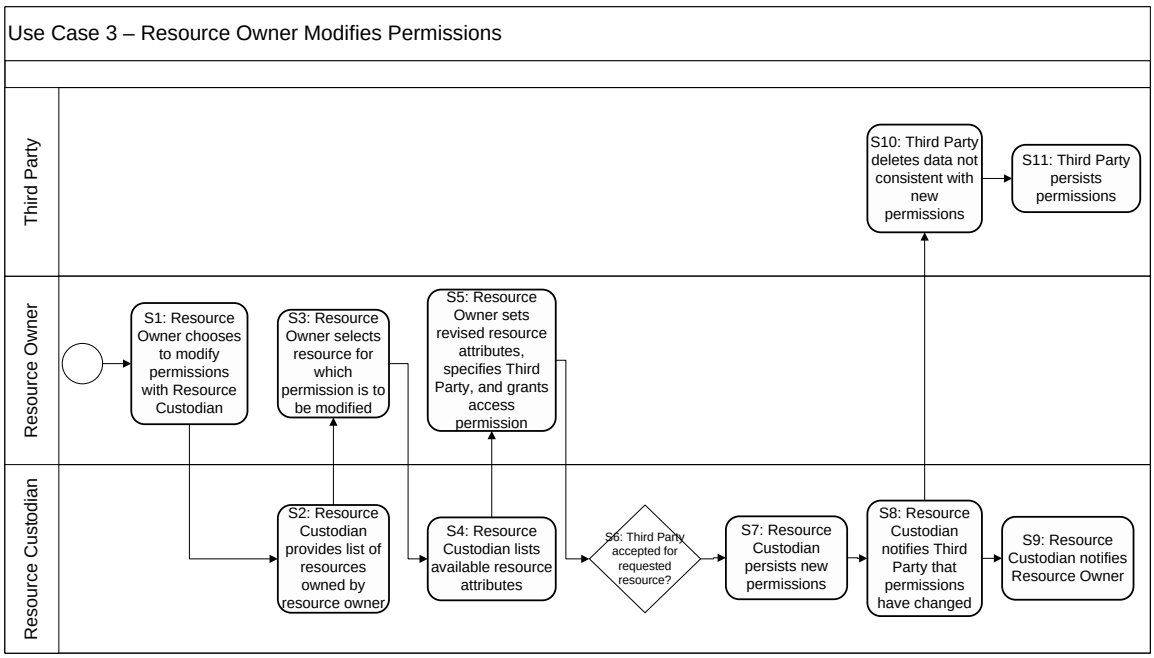

Diagram: Use Case 3

Main Success Scenario:

S1: Resource Owner chooses to modify relationship permissions with the Resource Custodian.

S2: Resource Custodian presents the Resource Owner with a list of resources that can be shared with Third Parties. If the Resource Owner only owns one resource, S2 and S3 may be skipped.

S3: Resource Owner chooses particular resource whose permissions he/she wishes to modify.

S4: Resource Custodian provides available resource attributes and current settings to Resource Owner.

S5: Resource Owner chooses new settings.

S6: The new permissions governing the relationship will apply only if the Resource Custodian accepts the selections for the Third Party (e.g., a Resource Custodian may constrain access to certain resource attributes depending on resource sensitivity).

S7: Resource Custodian persists the new permissions, which will be used from this point forward to govern the relationship (until further changed or the relationship is terminated).

S8: Resource Custodian notifies Third Party that permissions have changed (identifying the resource by its Shared Resource Key). This notification may be immediate or deferred (e.g., as part of a resource push from Use Case 8, perhaps as part of a header). No acknowledgement or confirmation is required.

S9: Resource Custodian notifies Resource Owner that permissions have been changed. No acknowledgment or confirmation is required.

S10: Third Party handles any data not consistent with the new permissions in the manner specified in any service agreements among the parties in the relationship.

S11: Third Party persists the new permissions, associating them with the Shared Resource Key.

2.4.4 Use Case 4: Resource Owner Terminates Relationship

Use Case Description: The Resource Owner has an existing third party data access relationship with a particular Resource Custodian and Third Party and wants to terminate that relationship.

Preconditions:

- Third Party has an established account with Resource Custodian.
- Resource Owner has established a third-party data access relationship with the Resource Custodian and the Third Party with respect to a particular resource, resulting in a unique Shared Resource Key identifying the relationship.

Minimal Guarantees:

No resource data or personal data is provided to the Third Party by the Resource Custodian as part of this interaction.

Success Guarantees:

- Both the Third Party and the Resource Custodian delete the Shared Resource Key for the relationship and no future interactions are permitted for that relationship.
- The Third Party handles any data not allowed by the termination of the relationship in the manner specified in any service agreements among the parties in the relationship (e.g., all instances of the data in control of the Third Party are deleted within a specified time frame).
- The Resource Custodian sends the Resource Owner confirmation of termination of the third-party data access relationship.

Trigger:

Resource Owner decides to terminate the third-party data access relationship that had allowed the Third Party to access specific resource data from a Resource Custodian.

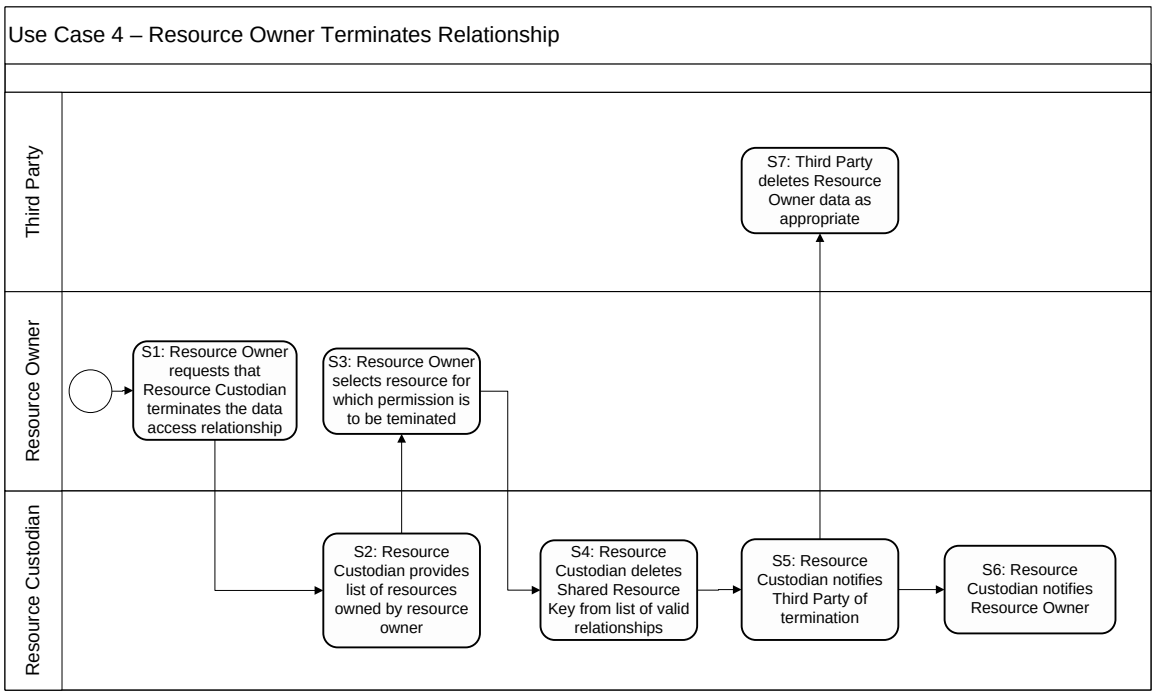

Diagram: Use Case 4

Main Success Scenario:

S1: Resource Owner requests that Resource Custodian terminate the data access relationship.

S2: Resource Custodian presents the Resource Owner with a list of resources for which there are valid relationships with Third Parties. If the Resource Owner only has one valid relationship, S2 and S3 may be skipped.

S3: Resource Owner chooses a resource whose relationship is to be terminated.

S4: Resource Custodian terminates the relationship, deleting the appropriate Shared Resource Key from its list of valid relationships.

S5: Resource Custodian notifies Third Party that the relationship has been terminated (identifying the relationship by its Shared Resource Key). No acknowledgement or confirmation is required.

S6: Resource Custodian notifies Resource Owner that the relationship has been terminated. No acknowledgment or confirmation is required.

S7: The Third Party handles any data not allowed by the termination of the relationship, in the manner specified in any service agreements among the parties in the relationship.

2.4.5 Use Case 5: Resource Custodian Terminates Relationship

Use Case Description: The Resource Owner has an existing third party data access relationship with a particular Resource Custodian and Third Party. The Resource Custodian wants to terminate the relationship (for whatever reason).

Preconditions:

- Third Party has an established account with Resource Custodian.
- Resource Owner has established a third-party data access relationship with the Resource Custodian and the Third Party with respect to a particular resource, resulting in a unique Shared Resource Key identifying the relationship.

Minimal Guarantees:

No resource data or personal data is provided to the Third Party by the Resource Custodian as part of this interaction.

Success Guarantees:

- Both the Third Party and the Resource Custodian delete the Shared Resource Key for the relationship and no future interactions are permitted for that relationship.
- The Third Party handles any data not allowed by the termination of the relationship, in the manner specified in any service agreements among the parties in the relationship (e.g., all instances of the data in control of the Third Party are deleted within a specified time frame).
- The Resource Custodian sends the Resource Owner notification of termination of the third-party data access relationship.

Trigger:

Resource Custodian decides to terminate a third party data access relationship with a Third Party.

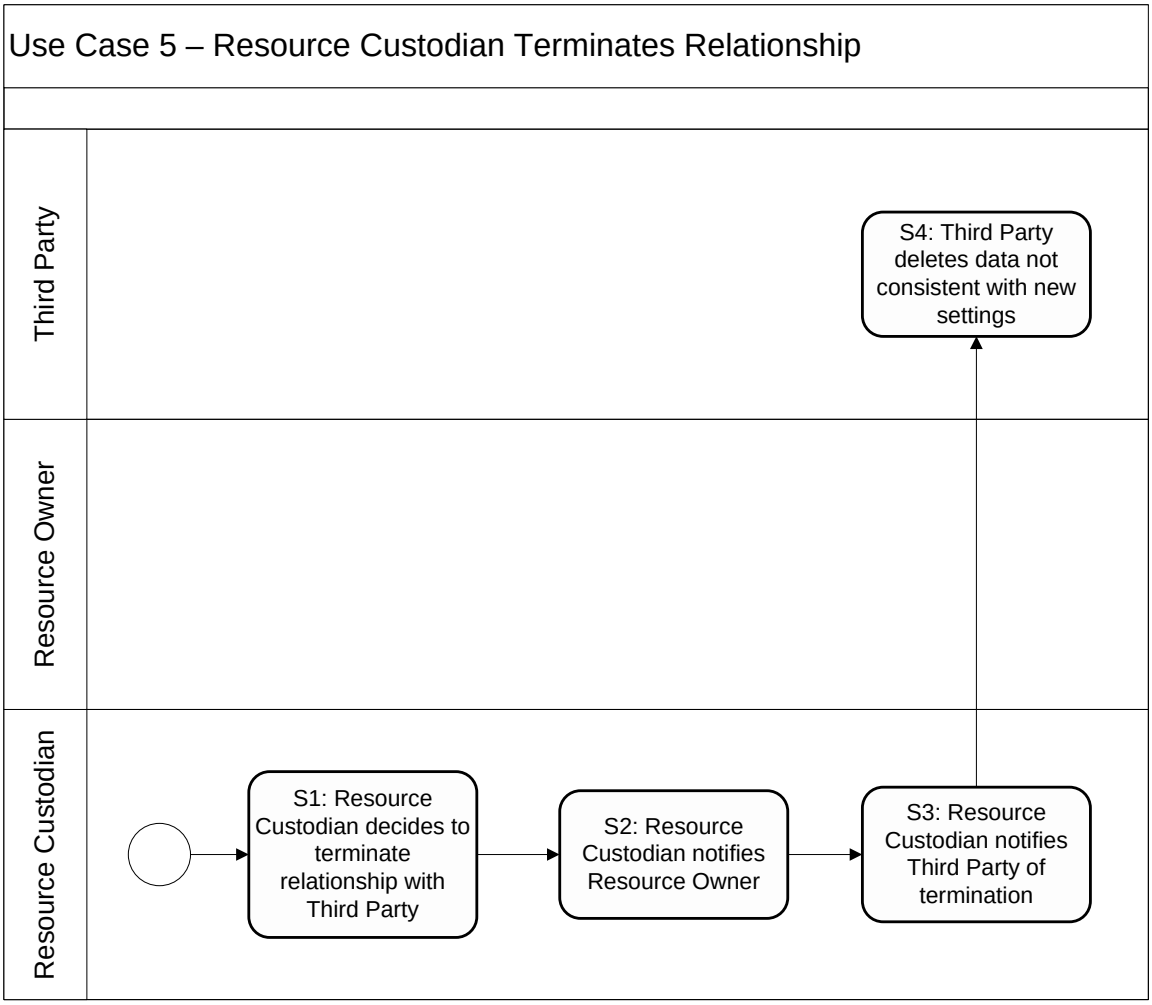

Diagram: Use Case 5

Main Success Scenario:

S1: Resource Custodian decides to terminate relationship with Third Party.

S2: Resource Custodian notifies Resource Owner of termination decision; no acknowledgement or confirmation is required.

S3: Resource Custodian notifies Third Party of termination of the relationship, identifying the relationship by a Shared Resource Key.

S4: The Third Party handles any data not allowed by the termination of the relationship, in the manner specified in any service agreements among the parties in the relationship.

2.4.6 Use Case 6: Third Party Terminates Relationship

Use Case Description: The Resource Owner has an existing third party data access relationship with a particular Resource Custodian and Third Party. The Third Party

determines that it no longer wants to provide services to the Resource Owner and terminates the relationship.

Preconditions:

- Third Party has an established account with Resource Custodian.
- Resource Owner has established a third-party data access relationship with the Resource Custodian and the Third Party with respect to a particular resource, resulting in a unique Shared Resource Key identifying the relationship.

Minimal Guarantees:

No resource data or personal data is provided to the Third Party by the Resource Custodian as part of this interaction.

Success Guarantees:

- Both the Third Party and the Resource Custodian delete the Shared Resource Key for the relationship and no future interactions are permitted for that relationship.
- The Third Party handles any data not allowed by the termination of the relationship, in the manner specified in any service agreements among the parties in the relationship (e.g., all instances of the data in control of the Third Party are deleted within a specified time frame).
- The Resource Custodian sends the Resource Owner notification of termination of the third-party data access relationship.

Trigger:

Third Party decides to terminate the relationship.

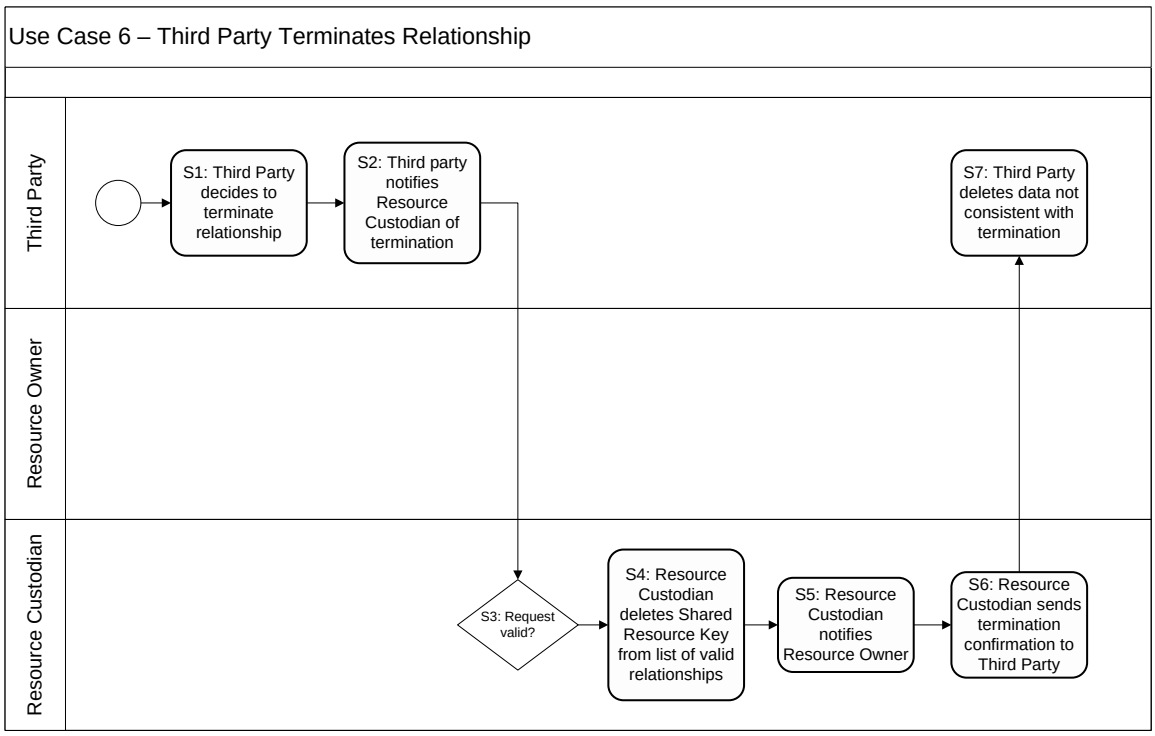

Diagram: Use Case 6

Main Success Scenario:

S1: Third Party decides to terminate a third party data access relationship.

S2: Third Party notifies Resource Custodian of termination of relationship, identifying the relationship by the Shared Resource Key.

S3: An invalid request (e.g., specification of a Shared Resource Key not associated with the Third Party) will not be accepted.

S4: Resource Custodian deletes Shared Resource Key, terminating the relationship.

S5: Resource Custodian notifies the Resource Owner of termination of the relationship. No acknowledgement or confirmation is required.

S6: Resource Custodian sends termination confirmation to Third Party.

S7: The Third Party handles any data not allowed by the termination of the relationship, in the manner specified in any service agreements among the parties in the relationship.

2.4.7 Use Case 7: Third Party Establishes Subscription with Resource Custodian

Use Case Description: The Resource Owner has an existing third party data access relationship with a particular Resource Custodian and Third Party. The Third Party establishes a *subscription* indicating the circumstances (i.e., an agreed-upon schedule

and/or specification of special events) under which the Resource Custodian should provide the Third Party with the relevant resource data.

Depending on the services offered by a Resource Custodian, the subscription may indicate the circumstances under which the Resource Custodian will send resource data or only notification that resource data is available (i.e., whether the Resource Custodian supports a push or pull model). Subscriptions may be parameterized, if supported by the Resource Custodian, to define preferred delivery criteria (e.g., new data whenever available or only once per day).

Preconditions:

- Third Party has an established account with Resource Custodian.
- Resource Owner has established a third-party data access relationship with the Resource Custodian and the Third Party with respect to a particular resource, resulting in a unique Shared Resource Key identifying the relationship.

Minimal Guarantees:

No resource data or personal data is provided to the Third Party by the Resource Custodian as part of this interaction.

Success Guarantees:

- The Resource Custodian records a valid subscription on behalf of the Third Party. Future data availability triggers satisfying the subscription will result in the appropriate information being sent to the Third Party (see Use Case 8 and Use Case 9 for examples of such information being sent).
- Resource Custodian sends the Third Party confirmation of its subscription request.
- Resource Custodian sends the Resource Owner notification of the Third Party's subscription request.

Trigger:

Third Party decides to establish a subscription for a Resource Owner's resource data with the Resource Custodian.

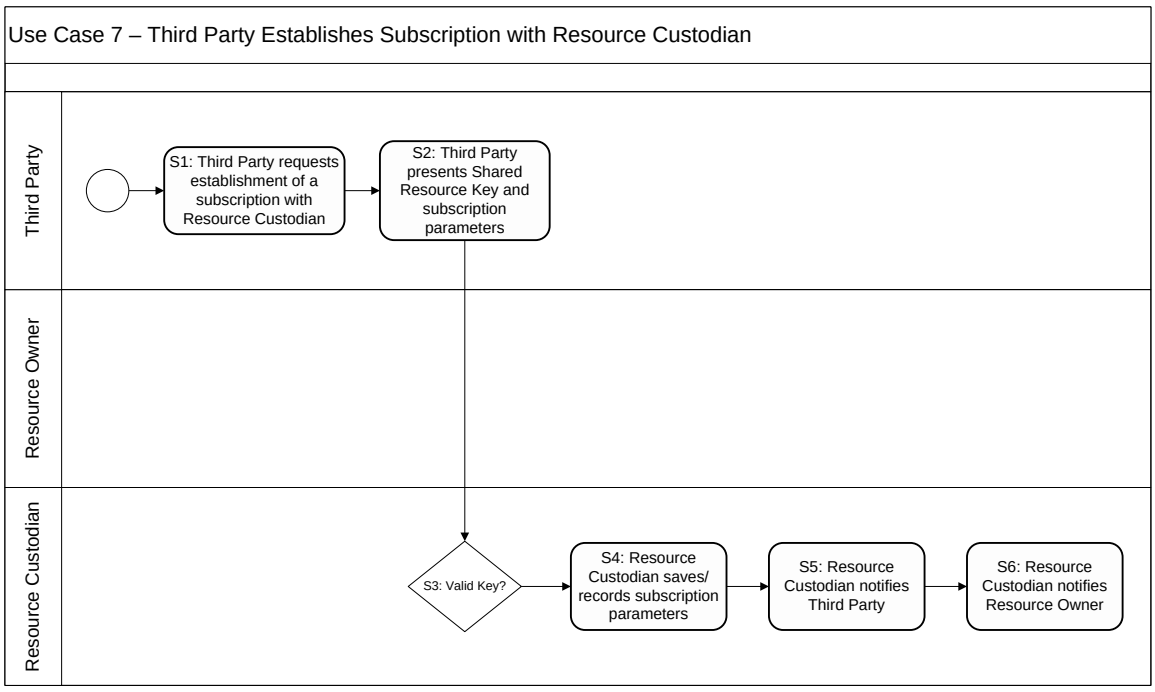

Diagram: Use Case 7

Main Success Scenario:

S1: Third Party requests that the Resource Custodian establish a new subscription.

S2: Third Party provides Resource Custodian with information defining the subscription request. At a minimum, this information includes a Shared Resource Key identifying the resource whose data is to be shared. The information may include additional subscription parameters, as supported by the Resource Custodian.

S3: The subscription will not be accepted if the Shared Resource Key is invalid.

S4: The Resource Custodian saves the subscription information, associating the subscription with the Shared Resource Key and the Third Party.

S5: The Resource Custodian notifies the Third Party that the subscription request was successful. No acknowledgement or confirmation is required.

S6: The Resource Custodian notifies the Resource Owner that the Third Party has completed a subscription for their resource data. No confirmation is required, as the Third Party already has permissions as indicated by the valid Shared Resource Key. If the subscription is not acceptable to the Resource Owner, Use Case 3 can be exercised to modify permissions for the Third Party.

2.4.8 Use Case 8: Resource Custodian Notifies Third Party of Resource Availability

Use Case Description: The Resource Owner has an existing third party data access relationship with a particular Resource Custodian and Third Party. The Third Party has established a subscription for receiving the relevant resource data from the Resource Custodian. A Third Party is notified when new data satisfying its subscription parameters is available.

Preconditions:

- Third Party has an established account with Resource Custodian.
- Resource Owner has established a third-party data access relationship with the Resource Custodian and the Third Party with respect to a particular resource, resulting in a unique Shared Resource Key identifying the relationship.
- Resource Custodian has resource data relevant to the Third Party.

Minimal Guarantees:

No personal information[6] is provided to the Third Party by the Resource Custodian.

Success Guarantees:

- The Resource Custodian has resource data (e.g., electricity usage data) that is available for access by the Third Party
- The Resource Custodian sends the Third Party notification of availability of resource data.

Trigger:

Conditions observable to the Resource Custodian change, causing a data availability trigger to be checked to see if there is a need to notify a Third Party of resource data availability. Such triggers can be caused by any of the following observable changes

- New resource data is received by the Resource Custodian
- A new subscription is received by the Resource Custodian
- A pre-defined interval has elapsed

[6] Personal information will be defined by the Resource Owner, Resources, Custodian and Third Party during service or contract discussions and will be guided by industry (national, international, and/or state) standards and regulations.

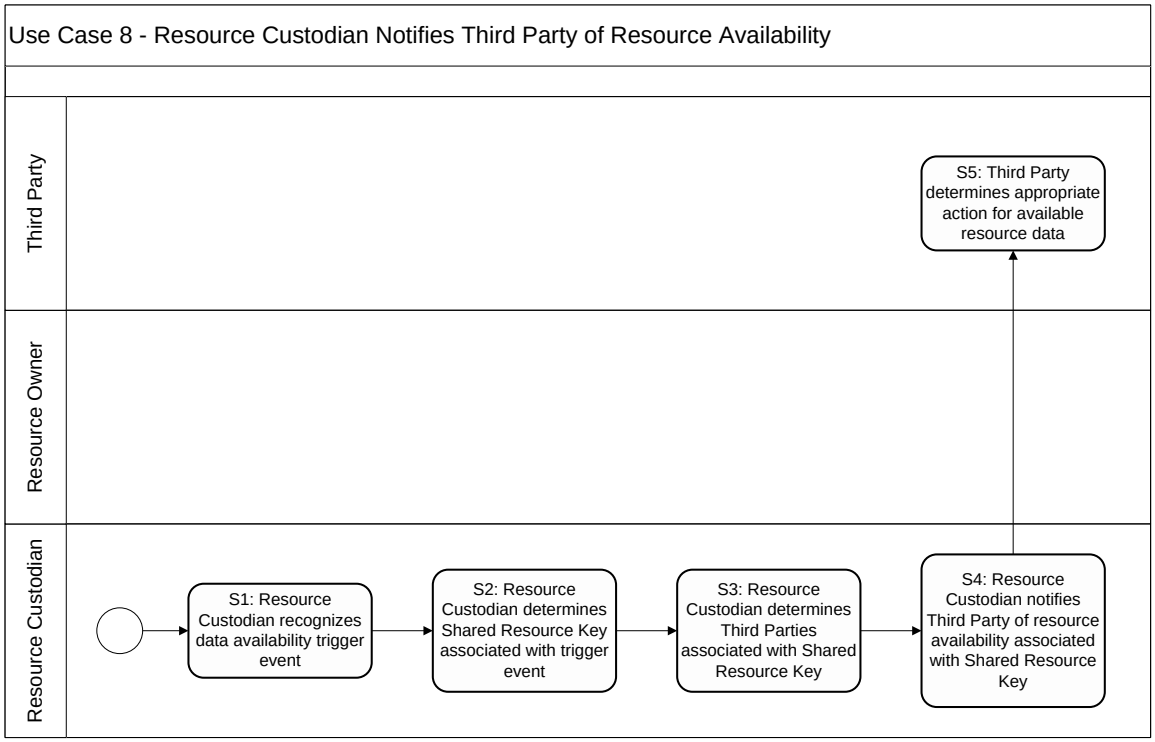

Diagram: Use Case 8

Main Success Scenario:

S1: A data availability trigger event is received by the Resource Custodian.

S2: Resource Custodian determines the Shared Resource Key associated with the data availability trigger. The Resource Custodian then determines if there are any subscriptions associated with the Shared Resource Key and whether the conditions of the subscription are satisfied (i.e., if it is time to notify a Third Party). If so, it proceeds to S3.

S3: Resource Custodian determines the Third Party associated with a satisfied subscription. This includes a check that the Third Party is still in a valid relationship with the Resource Custodian and any other relevant checks prior to determining that it is safe to send resource data to that Third Party

S4: Resource Custodian notifies the Third Party of the availability of resource data associated with the Shared Resource Key. Note that notification can take different forms. Notification could be sent asynchronously as soon as the trigger is evaluated. Notification for several resources could be bundled for delivery to a common Third Party. Notification could be queued, awaiting the next scheduled interaction with the Third Party (e.g., as part of a response to a regular pull from the Third Party). The essence of the use case is that a notification is prepared and delivered at some point; the specific mechanism and timing is not restricted.

S5: Third party determines the appropriate response. Typically, a Third Party will determine that it should retrieve the available data, using Use Case 10 (Section 2.4.10).

2.4.9 Use Case 9: Resource Custodian Sends (pushes) Resource to Third Party

Use Case Description: The Resource Owner has an existing third party data access relationship with a particular Resource Custodian and Third Party. The Third Party has established a subscription for receiving the relevant resource data from the Resource Custodian. This resource data is sent (pushed) to the subscribed Third Party by the Resource Custodian when an event triggers indicates a need to push new resource data.

Preconditions:

- Third Party has an established account with Resource Custodian.
- Resource Owner has established a third-party data access relationship with the Resource Custodian and the Third Party with respect to a particular resource, resulting in a unique Shared Resource Key identifying the relationship.
- A subscription by the Third Party to receive resource data from the Resource Custodian has been established.

Minimal Guarantees:

No personal information is provided to the Third Party by the Resource Custodian.

Success Guarantees:

- The Resource Custodian sends resource data to the subscribed Third Party.
- Only data specified in the subscription is sent to the Third Party.

Trigger:

Conditions observable to the Resource Custodian change, causing a data availability trigger to be checked to see if there is a need to push resource data to the Third Party. Such triggers can be caused by any of the following observable changes

- New resource data is received by the Resource Custodian
- A new subscription is received by the Resource Custodian
- A pre-defined interval has elapsed
- A request for resource data has been received from a Third Party

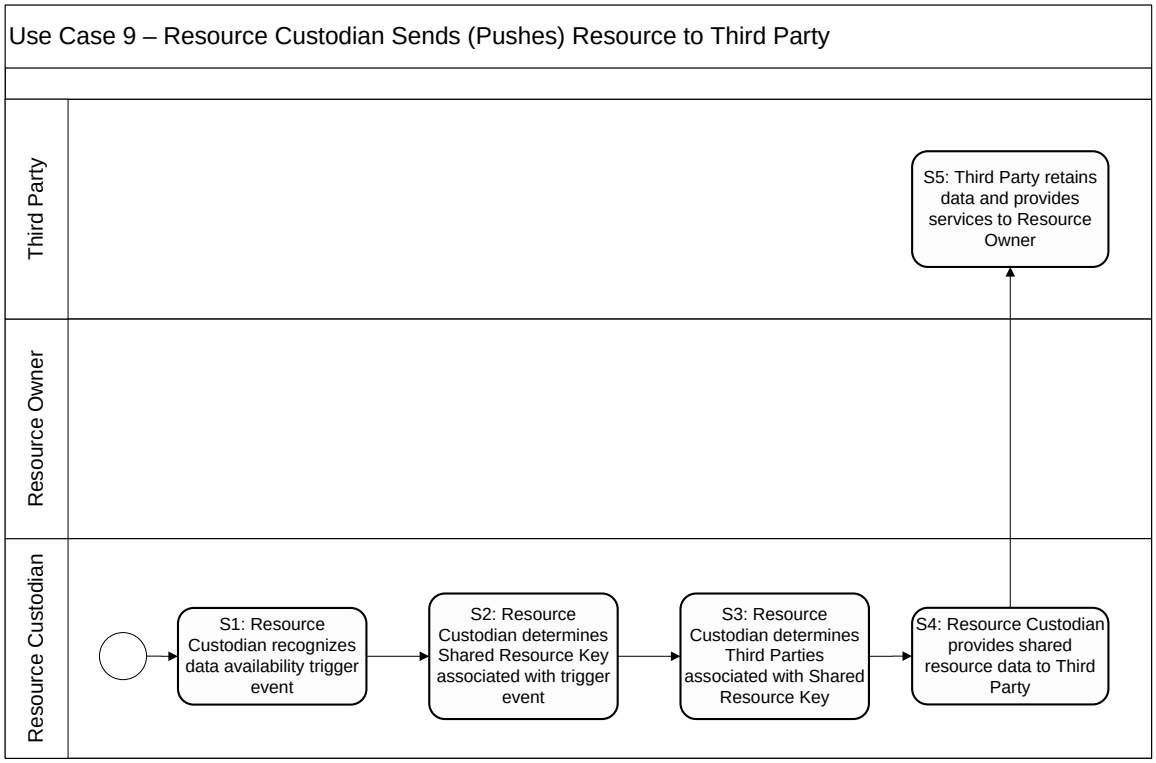

Diagram: Use Case 9

Main Success Scenario:

S1: A data availability trigger is received by the Resource Custodian.

S2: Resource Custodian determines the Shared Resource Key associated with the data availability trigger. It then determines if there are any subscriptions associated with the Shared Resource Key and whether the conditions of the subscription are satisfied (i.e., if it is time to send out resource data). If so, it proceeds to S3.

S3: Resource Custodian determines the Third Party associated with a satisfied subscription. This includes a check that the Third Party is still in a valid relationship with the Resource Custodian and any other relevant checks prior to releasing resource data to that Third Party.

S4: Resource Custodian provides shared resource data to Third Party.

S5: Third party persists data for the period specified by data retention requirements.[7]

[7] Data retention requirements will documented within the Resource Custodian, Resource Owner, and/or the Third Party and will be guided by industry (national, international, and/or state) standards and regulations.

2.4.10 Use Case 10: Third Party Receives (Pulls) Resource from Resource Custodian

Use Case Description: The Resource Owner has an existing third party data access relationship with a particular Resource Custodian and Third Party. The Third Party directly requests the relevant resource data from the Resource Custodian, which replies with the requested data if the request is valid.

Preconditions:

- Third Party has an established account with Resource Custodian.
- Resource Owner has established a third-party data access relationship with the Resource Custodian and the Third Party with respect to a particular resource, resulting in a unique Shared Resource Key identifying the relationship.
- Resource Custodian has resource data relevant to the Third Party.

Minimal Guarantees:

No personal data is provided to Third Parties by the Resource Custodian.

Success Guarantees:

- The Resource Custodian replies with the requested data.
- Only the requested resource data is provided by the Resource Custodian.

Trigger:

Third Party requests a resource data from Resource Custodian.

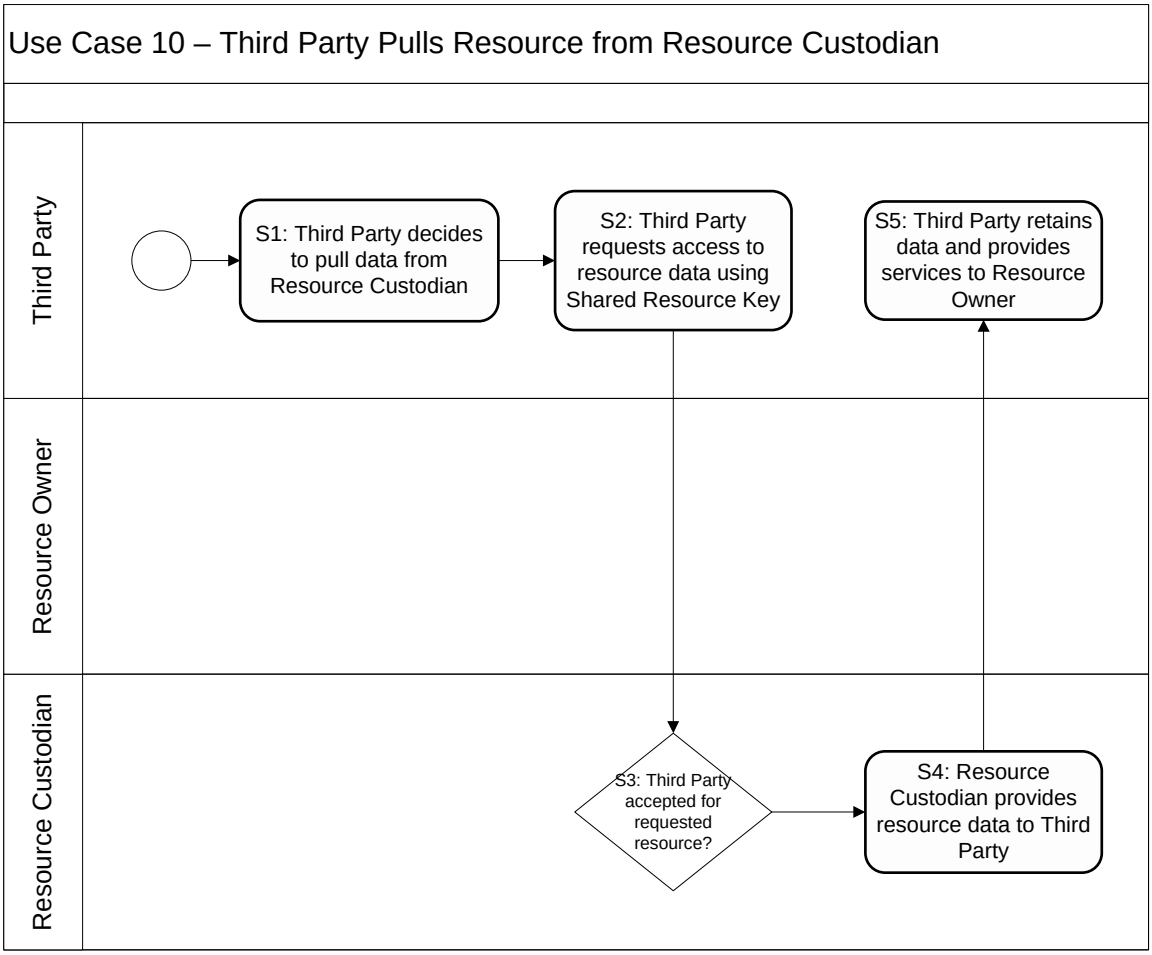

Diagram: Use Case 10

Main Success Scenario:

S1: Third Party decides to pull resource data from the Resource Custodian.

S2: Third Party specifies the resource data being requested. The request must contain the Shared Resource Key. It may also contain parameters (e.g., the period over which the specified data is requested), if permitted by Resource Custodian.

S3: Check validity of request (e.g., Shared Resource Key is still valid and registered with this Third Party or validity of any additional parameters).

S4: Resource Custodian sends requested resource data to Third Party.

S5: Third Party persists resource data for use in performing services for Resource Owner.

3 Control Mapping

This document asserts that certain controls are relevant to specific roles in the context of a use case or even specific use case steps. This section provides a link between the use cases described in Section 2.4 and the controls recommended in Section 4.

3.1 Mapping Controls to Roles

Application of controls to roles should be interpreted as follows:

- If a control refers to a system, it applies to the systems used in realizing each applicable role's responsibilities as identified in the use cases.
- If a control refers to an organization, it applies to the organization(s) implementing and operating the systems that realize the applicable roles.

Resource Owners will often be electric utility customers who do not use a custom system to participate in a third-party data access relationship. Instead, this role will often interact with the others using a simple web browser and little technological sophistication can be assumed. As such, few controls have been required of the Resource Owner role.

Table 1 - Controls to Roles Matrix lists all of the controls from the DHS catalog (U.S. Department of Homeland Security, 2009) and identifies the roles in the third-party data access pattern to which each applies. The Section column refers to numbering from the DHS catalog except where new controls were developed. New controls follow and append the DHS numbering and have been indicated as a "New ASAP Control" in the Description column. These include ASAP-2.6.12 and ASAP-2.11.7.

The markings in each cell should be interpreted as follows:

- **No marking**: this control is not a minimum requirement for this role for this profile
- **X**: this control is a minimum requirement for this role and the control applies as written across all use cases. This marking is typical for controls that are organizational in nature.
- **X***: this control is a minimum requirement for this role and the control applies as written, but only to specified steps from the use cases. This marking is typical of technical controls.
- **M**: this control is a minimum requirement for this role and the control applies as modified in this document. The control applies across all use cases.
- **M***: this control is a minimum requirement for this role and the control applies as modified in this document. The control only applies to specified steps from the use cases.

For those controls that apply only to specified steps of the use cases, see Tables 2-7 to determine the applicable steps for each role from the third-party data access pattern.

Table 1 - Controls to Roles Matrix

Section	Description	Resource Custodian	Third Party	Resource Owner
2.1	Security Policy			
2.1.1	Security Policy and Procedures	X	X	
2.2	Organizational Security			
2.2.1	Management Policy and Procedures	X	X	
2.2.2	Management Accountability	X	X	
2.2.3	Baseline Practices	X	X	
2.2.4	Coordination of Threat Mitigation	X	X	
2.2.5	Security Policies for Third Parties	X		
2.2.6	Termination of Third-Party Access	X		X
2.3	Personnel Security			
2.3.1	Personnel Security Policy and Procedures	X	X	
2.3.2	Position Categorization	X	X	
2.3.3	Personnel Screening	X	X	
2.3.4	Personnel Termination	X	X	
2.3.5	Personnel Transfer	X	X	
2.3.6	Access Agreements	X	X	X
2.3.7	Third-Party Personnel Security	X		X
2.3.8	Personnel Accountability	X	X	
2.3.9	Personnel Roles	X	X	
2.4	Physical and Environmental Security			

Section	Description	Resource Custodian	Third Party	Resource Owner
2.4.1	Physical and Environmental Security Policy and Procedures	X	X	
2.4.2	Physical Access Authorizations	X	X	
2.4.3	Physical Access Control	X	X	
2.4.4	Monitoring Physical Access	X	X	
2.4.5	Visitor Control	X	X	
2.4.6	Visitor Records	X	X	
2.4.7	Physical Access Log Retention	X	X	
2.4.8	Emergency Shutoff	X	X	
2.4.9	Emergency Power	X	X	
2.4.10	Emergency Lighting	X	X	
2.4.11	Fire Protection	X	X	
2.4.12	Temperature and Humidity Controls	X	X	
2.4.13	Water Damage Protection	X	X	
2.4.14	Delivery and Removal	X	X	
2.4.15	Alternate Work Site	X	X	
2.4.16	Portable Media	X	X	
2.4.17	Personnel and Asset Tracking	X	X	
2.4.18	Location of Control System Assets	X	X	
2.4.19	Information Leakage	X	X	
2.4.20	Power Equipment and Power Cabling	X	X	
2.4.21	Physical Device Access Control	X	X	
2.5	System and Services Acquisition			
2.5.1	System and Services Acquisition Policy and Procedures	X	X	
2.5.2	Allocation of Resources	X	X	
2.5.3	Life-Cycle Support	X	X	
2.5.4	Acquisitions	X	X	
2.5.5	Control System Documentation	X	X	
2.5.6	Software License Usage Restrictions	X	X	
2.5.7	User-Installed Software	X	X	
2.5.8	Security Engineering Principles	X	X	
2.5.9	Outsourced Control System Services	X	X	
2.5.10	Vendor Configuration Management	X	X	
2.5.11	Vendor Security Testing	X	X	
2.5.12	Supply Chain Protection	X	X	
2.5.13	Trustworthiness	X	X	
2.6	Configuration Management			
2.6.1	Configuration Management Policy and Procedures	M	M	
2.6.2	Baseline Configuration	M	M	
2.6.3	Configuration Change Control	M	M	

Section	Description	Resource Custodian	Third Party	Resource Owner
2.6.4	Monitoring Configuration Changes	M	M	
2.6.5	Access Restrictions for Configuration Change	X	X	
2.6.6	Configuration Settings	M	M	
2.6.7	Configuration for Least Functionality	X	X	
2.6.8	Configuration Assets	M	M	
2.6.9	Addition, Removal, and Disposal of Equipment	M	M	
2.6.10	Factory Default Authentication Management	M	M	
2.6.11	Configuration Management Plan	M	M	
2.6.12	Customer Configuration Management (New ASAP Control)			M
2.7	Strategic Planning			
2.7.1	Strategic Planning Policy and Procedures	X	X	
2.7.2	Control System Security Plan	X	X	
2.7.3	Interruption Identification and Classification	X	X	
2.7.4	Roles and Responsibilities	X	X	
2.7.5	Planning Process Training	X	X	
2.7.6	Testing	X	X	
2.7.7	Investigate and Analyze	X	X	
2.7.8	Corrective Action	X	X	
2.7.9	Risk Mitigation	X	X	
2.7.10	System Security Plan Update	X	X	
2.7.11	Rules of Behavior	X	X	
2.7.12	Security-Related Activity Planning	X	X	
2.8	System and Communication Protection			
2.8.1	System and Communication Protection Policy and Procedures	X	X	
2.8.2	Management Port Partitioning	X	X	
2.8.3	Security Function Isolation	X	X	
2.8.4	Information Remnants	X	X	
2.8.5	Denial-of-Service Protection	X	X	
2.8.6	Resource Priority	X	X	
2.8.7	Boundary Protection	X	X	
2.8.8	Communication Integrity	X	X	
2.8.9	Communication Confidentiality	X	X	
2.8.10	Trusted Path	X	X	
2.8.11	Cryptographic Key Establishment and Management	X	X	
2.8.12	Use of Validated Cryptography	X	X	
2.8.13	Collaborative Computing	X	X	
2.8.14	Transmission of Security Parameters	X	X	
2.8.15	Public Key Infrastructure Certificates	X	X	
2.8.16	Mobile Code	X	X	

Section	Description	Resource Custodian	Third Party	Resource Owner
2.8.17	Voice-Over Internet Protocol	X	X	
2.8.18	System Connections	X	X	
2.8.19	Security Roles	X	X	
2.8.20	Message Authenticity	X	X	
2.8.21	Architecture and Provisioning for Name/Address Resolution Service	X	X	
2.8.22	Secure Name/Address Resolution Service (Authoritative Source)	X	X	
2.8.23	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	X	X	
2.8.24	Fail in Known State			
2.8.25	Thin Nodes			
2.8.26	Honeypots			
2.8.27	Operating System-Independent Applications			
2.8.28	Confidentiality of Information at Rest			
2.8.29	Heterogeneity			
2.8.30	Virtualization Techniques			
2.8.31	Covert Channel Analysis			
2.9	Information and Document Management			
2.9.1	Information and Document Management Policy and Procedures	M*	M*	M*
2.9.2	Information and Document Retention	M*	M*	M*
2.9.3	Information Handling	M*	M*	M*
2.9.4	Information Classification	X*	X*	X*
2.9.5	Information Exchange	X*	X*	X*
2.9.6	Information and Document Classification	X*	X*	X*
2.9.7	Information and Document Retrieval	X*	X*	X*
2.9.8	Information and Document Destruction	M*	M*	
2.9.9	Information and Document Management Review	M*	M*	M*
2.9.10	Automated Marking	X*	X*	X*
2.9.11	Automated Labeling	X*	X*	X*
2.10	System Development and Maintenance			
2.10.1	System Maintenance Policy and Procedures			
2.10.2	Legacy System Upgrades			
2.10.3	System Monitoring and Evaluation			
2.10.4	Backup and Recovery	M*	M*	
2.10.5	Unplanned System Maintenance			
2.10.6	Periodic System Maintenance			
2.10.7	Maintenance Tools			
2.10.8	Maintenance Personnel			
2.10.9	Remote Maintenance			
2.10.10	Timely Maintenance			

Section	Description	Resource Custodian	Third Party	Resource Owner
2.11	Security Awareness and Training			
2.11.1	Security Awareness and Training Policy and Procedures	M	M	
2.11.2	Security Awareness	M	M	
2.11.3	Security Training	M	M	
2.11.4	Security Training Records	M	M	
2.11.5	Contact with Security Groups and Associations	M	M	
2.11.6	Security Responsibility Testing	M	M	
2.11.7	Customer Awareness and Education (New ASAP Control)	M	M	
2.12	Incident Response			
2.12.1	Incident Response Policy and Procedures	X	X	
2.12.2	Continuity of Operations Plan	X	X	
2.12.3	Continuity of Operations Roles and Responsibilities	X	X	
2.12.4	Incident Response Training	X	X	
2.12.5	Continuity of Operations Plan Testing	X	X	
2.12.6	Continuity of Operations Plan Update	X	X	
2.12.7	Incident Handling	X	X	
2.12.8	Incident Monitoring	X	X	
2.12.9	Incident Reporting	X	X	
2.12.10	Incident Response Assistance	X	X	
2.12.11	Incident Response Investigation and Analysis	X	X	
2.12.12	Corrective Action	X	X	
2.12.13	Alternate Storage Sites	X	X	
2.12.14	Alternate Command/Control Methods	X	X	
2.12.15	Alternate Control Center	X	X	
2.12.16	Control System Backup	X	X	
2.12.17	Control System Recovery and Reconstitution	X	X	
2.12.18	Fail-Safe Response	X	X	
2.13	Media Protection			
2.13.1	Media Protection Policy and Procedures	X	X	
2.13.2	Media Access	X	X	
2.13.3	Media Classification	X	X	
2.13.4	Media Marking	X	X	
2.13.5	Media Storage	X	X	
2.13.6	Media Transport	X	X	
2.13.7	Media Sanitization and Disposal	X	X	
2.14	System and Information Integrity			
2.14.1	System and Information Integrity Policy and Procedures	X	X	
2.14.2	Flaw Remediation	M	M	
2.14.3	Malicious Code Protection	M	M	

Section	Description	Resource Custodian	Third Party	Resource Owner
2.14.4	System Monitoring Tools and Techniques	M	M	
2.14.5	Security Alerts and Advisories	X	X	
2.14.6	Security Functionality Verification	X	X	
2.14.7	Software and Information Integrity	X	X	
2.14.8	Spam Protection	X	X	
2.14.9	Information Input Restrictions	X*	X*	
2.14.10	Information Input Accuracy, Completeness, Validity, and Authenticity	X*	X*	
2.14.11	Error Handling	M	M	
2.14.12	Information Output Handling and Retention	M*		
2.14.13	Predictable Failure Prevention	X	X	
2.15	Access Control			
2.15.1	Access Control Policy and Procedures	X	X	
2.15.2	Identification and Authentication Policy and Procedures	X	X	
2.15.3	Account Management	X	X	
2.15.4	Identifier Management	X	X	
2.15.5	Authenticator Management	X	X	
2.15.6	Account Review	X	X	
2.15.7	Access Enforcement	X*	X*	
2.15.8	Separation of Duties	M*	M*	
2.15.9	Least Privilege	M	M	
2.15.10	User Identification and Authentication	X*	X*	
2.15.11	Permitted Actions without Identification or Authentication	X*	X*	
2.15.12	Device Identification and Authentication	X*	X*	
2.15.13	Authenticator Feedback	X*	X*	
2.15.14	Cryptographic Module Authentication	X*	X*	
2.15.15	Information Flow Enforcement	X*	X*	
2.15.16	Passwords	X	X	
2.15.17	System Use Notification	X	X	
2.15.18	Concurrent Session Control	X	X	
2.15.19	Previous Logon Notification	X	X	
2.15.20	Unsuccessful Login Attempts	X	X	
2.15.21	Session Lock	X	X	
2.15.22	Remote Session Termination	X	X	
2.15.23	Remote Access Policy and Procedures	X	X	
2.15.24	Remote Access	X	X	
2.15.25	Access Control for Portable and Mobile Devices	X	X	
2.15.26	Wireless Access Restrictions	X	X	
2.15.27	Personally Owned Information	X	X	
2.15.28	External Access Protections	X	X	

Section	Description	Resource Custodian	Third Party	Resource Owner
2.15.29	Use of External Information Control Systems	X	X	
2.16	Audit and Accountability			
2.16.1	Audit and Accountability Policy and Procedures	M	M	M
2.16.2	Auditable Events	M	M	M
2.16.3	Content of Audit Records	X	X	X
2.16.4	Audit Storage Capacity	X	X	X
2.16.5	Response to Audit Processing Failures	X	X	X
2.16.6	Audit Monitoring, Analysis, and Reporting	M	M	M
2.16.7	Audit Reduction and Report Generation	M	M	M
2.16.8	Time Stamps	X*	X*	X*
2.16.9	Protection of Audit Information			
2.16.10	Audit Record Retention	X	X	X
2.16.11	Conduct and Frequency of Audits	M	M	M
2.16.12	Auditor Qualification	M	M	M
2.16.13	Audit Tools			
2.16.14	Security Policy Compliance	X	X	X
2.16.15	Audit Generation	X	X	X
2.17	Monitoring and Reviewing Control System Security Policy			
2.17.1	Monitoring and Reviewing Control System Security Management Policy and Procedures	X	X	
2.17.2	Continuous Improvement	X	X	
2.17.3	Monitoring of Security Policy	X	X	
2.17.4	Best Practices	X	X	
2.17.5	Security Accreditation	X	X	
2.17.6	Security Certification	X	X	
2.18	Risk Management and Assessment			
2.18.1	Risk Assessment Policy and Procedures	X	X	
2.18.2	Risk Management Plan	X	X	
2.18.3	Certification, Accreditation, and Security Assessment Policies and Procedures	X	X	
2.18.4	Security Assessments	X	X	
2.18.5	Control System Connections	X	X	
2.18.6	Plan of Action and Milestones	X	X	
2.18.7	Continuous Monitoring	X	X	
2.18.8	Security Categorization			
2.18.9	Risk Assessment	X	X	
2.18.10	Risk Assessment Update	X	X	
2.18.11	Vulnerability Assessment and Awareness	X	X	
2.18.12	Identify, Classify, Prioritize, and Analyze Potential Security Risks	X	X	
2.19	Security Program Management			

Section	Description	Resource Custodian	Third Party	Resource Owner
2.19.1	Security Program Plan			
2.19.2	Senior Security Officer			
2.19.3	Security Resources			
2.19.4	Plan of Action and Milestones Process			
2.19.5	System Inventory			
2.19.6	Security Measures of Performance			
2.19.7	Enterprise Architecture	X	X	
2.19.8	Critical Infrastructure Plan			
2.19.9	Risk Management Strategy	X	X	
2.19.10	Security Authorization Process			
2.19.11	Mission/Business Process Definition			

3.2 Mapping Controls to Use Case Steps

Recommendations for applying controls to specific steps in the use cases appear in the following tables. (Note that two tables are provided per role, due to space restrictions.) The markings in each cell should be interpreted with respect to the identified role for that table as follows:

- **No marking**: this control is not recommended for application to this step in the use case.
- **X**: this control applies to this step without modification.

Rows in these tables are only provided for controls that apply to specific use case steps (i.e., those controls marked in Table 1 with an X* or M*). As such, gaps in the numbering are to be expected.

Table 2 – Recommended Control Application for Resource Custodians (Use Cases 1-4)

Resource Custodian																																				
	Use Case 1									Use Case 2									Use Case 3											Use Case 4						
Section	1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7	8	9	10	11	1	2	3	4	5	6	7
2.9.1	X				X	X						X			X	X			X						X	X	X			X			X	X	X	
2.9.2	X				X	X						X			X	X			X						X	X	X			X			X	X	X	
2.9.3	X				X	X						X			X	X			X						X	X	X			X			X	X	X	
2.9.4	X				X	X						X			X	X			X						X	X	X			X			X	X	X	
2.9.5	X					X						X			X	X			X							X	X			X				X	X	
2.9.6	X				X	X						X			X	X			X						X	X	X			X			X	X	X	
2.9.7	X				X	X						X			X	X			X						X	X	X			X			X	X	X	
2.9.8																																	X			

Resource Custodian

	Use Case 1									Use Case 2									Use Case 3											Use Case 4						
Section	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
2.9.9	X				X	X						X			X	X			X						X	X	X			X			X	X	X	
2.9.10	X				X	X						X			X	X			X						X	X	X			X			X	X	X	
2.9.11	X				X	X						X			X	X			X						X	X	X			X			X	X	X	
2.10.4					X										X										X								X			
2.14.9	X		X									X		X					X		X		X							X		X				
2.14.10	X		X	X								X		X					X		X		X	X						X		X				
2.14.12					X										X																						
2.15.7	X						X					X							X											X						
2.15.8	X	X	X	X	X	X						X	X	X	X	X	X		X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	
2.15.9	X	X	X	X	X	X						X	X	X	X	X	X		X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	
2.15.10	X											X							X											X						
2.15.11	X											X							X											X						
2.15.12																										X								X			
2.15.13	X											X							X											X						
2.15.14	X											X							X							X				X						
2.15.15	X	X	X	X	X	X						X	X	X	X	X	X		X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	
2.16.8	X	X	X	X	X	X						X	X	X	X	X	X		X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	

Table 3 - Recommended Control Application for Resource Custodians (Use Cases 5-10)

Resource Custodian																															
	Use Case 5				Use Case 6							Use Case 7						Use Case 8					Use Case 9					Use Case 10				
Section	1	2	3	4	1	2	3	4	5	6	7	1	2	3	4	5	6	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
2.9.1		X	X			X		X	X	X		X			X	X	X				X					X		X			X	
2.9.2		X	X			X		X	X	X		X			X	X	X				X					X		X			X	
2.9.3		X	X			X		X	X	X		X			X	X	X				X					X		X			X	
2.9.4		X	X			X		X	X	X		X			X	X	X				X					X		X			X	
2.9.5		X	X			X			X	X		X				X	X				X					X		X			X	
2.9.6		X	X			X		X	X	X		X			X	X	X				X					X		X			X	
2.9.7		X	X			X		X	X	X		X			X	X	X				X					X		X			X	
2.9.8								X																								
2.9.9		X	X			X		X	X	X		X			X	X	X				X					X		X			X	
2.9.10		X	X			X		X	X	X		X			X	X	X				X					X		X			X	
2.9.11		X	X			X		X	X	X		X			X	X	X				X					X		X			X	
2.10.4				X				X							X																	
2.14.9						X						X	X															X	X			
2.14.10						X	X					X	X	X														X	X	X		
2.14.12																										X					X	
2.15.7						X						X																X	X			
2.15.8	X	X	X			X	X	X	X	X		X	X	X	X													X	X		X	
2.15.9	X	X	X			X	X	X	X	X		X	X	X	X													X	X		X	
2.15.10						X						X																X				

Resource Custodian																															
	Use Case 5				Use Case 6							Use Case 7						Use Case 8					Use Case 9					Use Case 10				
Section	1	2	3	4	1	2	3	4	5	6	7	1	2	3	4	5	6	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
2.15.11						X						X																X				
2.15.12			X							X			X	X							X						X		X	X	X	
2.15.13						X						X																X				
2.15.14						X						X																X				
2.15.15	X	X	X			X	X	X	X	X		X	X	X	X													X	X	X	X	
2.16.8		X	X			X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Table 4 - Recommended Control Application for Third Parties (Use Cases 1-4)

Third Party																																	
	Use Case 1									Use Case 2										Use Case 3											Use Case 4						
Section	1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7	8	9	10	11	1	2	3	4	5	6	7
2.9.1								X	X									X										X	X							X
2.9.2								X	X									X										X	X							X
2.9.3								X	X									X										X	X							X
2.9.4								X	X									X										X	X							X
2.9.5								X										X										X								X
2.9.6								X	X									X										X	X							X
2.9.7								X	X									X										X	X							X

Third Party																																			
	Use Case 1									Use Case 2									Use Case 3											Use Case 4						
Section	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
2.9.8																												X								X
2.9.9								X	X									X										X	X							X
2.9.10								X	X									X										X	X							X
2.9.11								X	X									X										X	X							X
2.10.4									X									X										X	X							X
2.14.9							X	X		X							X								X									X		
2.14.10							X	X		X							X								X									X		
2.15.7							X			X							X								X									X		
2.15.8											X																	X								X
2.15.9											X																	X								X
2.15.10							X			X							X								X									X		
2.15.11										X																										
2.15.12																										X									X		
2.15.13							X			X							X								X									X		
2.15.14							X			X							X								X									X		
2.15.15								X	X	X	X						X	X							X		X	X						X		X
2.16.8							X	X	X	X	X	X					X	X							X		X	X						X		X

Table 5 - Recommended Control Application for Third Parties (Use Cases 5-10)

Third Party																														
	Use Case 5				Use Case 6							Use Case 7						Use Case 8					Use Case 9					Use Case 10				
Section	1	2	3	4	1	2	3	4	5	6	7	1	2	3	4	5	6	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
2.9.1				X		X					X		X			X						X					X		X			X
2.9.2				X		X					X		X			X						X					X		X			X
2.9.3				X		X					X		X			X						X					X		X			X
2.9.4				X		X					X		X			X						X					X		X			X
2.9.5				X		X					X		X			X						X					X		X			X
2.9.6				X		X					X		X			X						X					X		X			X
2.9.7				X		X					X		X			X						X					X		X			X
2.9.8				X							X											X										
2.9.9				X		X					X		X			X						X					X		X			X
2.9.10				X		X					X		X			X						X					X		X			X
2.9.11				X		X					X		X			X						X					X		X			X
2.10.4				X							X											X					X					X
2.14.9			X																		X					X				X		
2.14.10			X																		X					X				X		
2.15.7			X								X										X					X				X		
2.15.8				X	X	X					X	X	X									X					X					X
2.15.9				X	X	X					X	X	X									X					X					X
2.15.10			X								X										X					X				X		
2.15.11																																

Third Party																														
	Use Case 5				Use Case 6							Use Case 7						Use Case 8					Use Case 9					Use Case 10				
Section	1	2	3	4	1	2	3	4	5	6	7	1	2	3	4	5	6	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
2.15.12			X							X			X	X							X					X					X	
2.15.13			X								X										X					X					X	
2.15.14			X								X										X					X					X	
2.15.15			X	X	X	X					X	X	X								X	X				X	X	X	X			X
2.16.8				X		X	X			X	X	X	X	X		X					X	X				X	X	X	X	X	X	X

Table 6 - Recommended Control Application for Resource Owners (Use Cases 1-4)

Resource Owner																																		
	Use Case 1									Use Case 2										Use Case 3												Use Case 4						
Section	1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7	8	9	10	11	1	2	3	4	5	6	7
2.9.1							X	X									X										X								X	
2.9.2							X	X									X										X								X	
2.9.3							X	X									X										X								X	
2.9.4							X	X									X										X								X	
2.9.5							X	X									X										X								X	
2.9.6							X	X									X										X								X	
2.9.7							X	X									X										X								X	
2.9.9							X	X									X										X								X	
2.9.10							X	X									X										X								X	

Resource Owner																																					
	Use Case 1									Use Case 2									Use Case 3											Use Case 4						
Section	1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7	8	9	10	11	1	2	3	4	5	6	7
2.9.11							X	X									X										X										
2.16.8	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X		X	X	X	X	X	X			X			X	X	X	X		X	

Table 7 - Recommended Control Application for Resource Owners (Use Cases 5-10)

Resource Owner																																					
	Use Case 5				Use Case 6							Use Case 7						Use Case 8					Use Case 9					Use Case 10										
Section	1	2	3	4	1	2	3	4	5	6	7	1	2	3	4	5	6	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5					
2.9.1		X							X								X																				
2.9.2		X							X								X																				
2.9.3		X							X								X																				
2.9.4		X							X								X																				
2.9.5		X							X								X																				
2.9.6		X							X								X																				
2.9.7		X							X								X																				
2.9.9		X							X								X																				
2.9.10		X							X								X																				
2.9.11		X							X								X																				
2.16.8		X							X								X																				

4 Modified Controls

The controls in this document are primarily drawn from the DHS Catalog of Control Systems Security: Recommendations for Standards Developers (U.S. Department of Homeland Security, 2009), with the addition of new controls to fill gaps specific to this security profile. Many of the controls from the DHS catalog apply with little or no modification. We interpret each control that specifies a "control system" as also applying to "information systems" involved in third-party data access.

Some controls originating with the DHS recommendations require modification or clarification to explain how they apply in the context of third-party data access. Those controls that have been modified appear in this section with new text.

See Table 1 for a summary of which controls apply to which roles. See Table 2 through Table 7 for a mapping of some of these controls to the specific use case steps at which they apply (other controls apply equally across all use cases).

DHS-2.6 Configuration Management

The organization’s security program needs to implement policies and procedures that create a process by which the organization manages and documents all configuration changes to the system. Comprehensive change and configuration management processes needs to be implemented and used to ensure that only approved and tested changes are made to the system configuration. Systems need to be configured properly to maintain optimal operation. Therefore, only tested and approved changes should be allowed on a system. Vendor updates and patches need to be thoroughly tested on a nonproduction system setup before being introduced into the production environment to ensure no

adverse effects occur. Configuration requirements need to be identified, conveyed to the appropriate party, and enforced or confirmed, for software that accesses or interoperates with the organization's system but is not controlled by the organization (e.g., Resource Owner web browsers and devices, other organizations' systems and applications).

DHS-2.6.1 Configuration Management Policy and Procedures

DHS-2.6.1.1 Requirement

The organization develops, disseminates, and periodically reviews and updates:

1. A formal, documented configuration management policy that addresses:
    a. The purpose of the configuration management policy as it relates to protecting the organization's personnel and assets
    b. The scope of the configuration management policy as it applies to all the organizational staff and third-party contractors.
    c. The roles, responsibilities, management accountability structure, and coordination among organizational entities contained in the configuration management policy to ensure compliance with the organization's security policy and other regulatory commitments
2. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls
3. The personnel qualification levels required to make changes, the conditions under which changes are allowed, and what approvals are required for those changes.

DHS-2.6.1.2 Supplemental Guidance

The organization ensures the configuration management policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general system security policy for the organization. Configuration management procedures can be developed for the security program in general and for a particular system component when required.

Configuration requirements must be conveyed to the appropriate party, and enforced or confirmed, for software that accesses or interoperates with the organization's system but is not in the direct control of the organization (e.g., Resource Owner web browsers and devices, other organizations' systems and applications).

DHS-2.6.1.3 Requirement Enhancements

None.

DHS-2.6.1.4Third Party Data Access4 Rationale

This requirement is a widely recognized best practice. It has been expanded from the original DHS control to emphasize the need to include configuration requirements for software that accesses or interoperate with the organization's systems, even when that software is not in the direct control of the organization.

DHS-2.6.2 Baseline Configuration

DHS-2.6.2.1 Requirement

The organization develops, documents, and maintains a current baseline configuration of the system and an inventory of the system's constituent components. This includes a list of software (with configuration settings) that access or interoperate with the organization's system, to include external systems not in the direct control of the organization.

DHS-2.6.2.2 Supplemental Guidance

This control establishes a baseline configuration for the system. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the system architecture. The baseline configuration also provides the organization with a well-defined and documented specification to which the system is built, and deviations, if required, are documented in support of mission needs/objectives. The configuration of the system component should be consistent with the organization's system architecture and documentation policy. The inventory of system components includes information (e.g., manufacturer, type, serial number, version number, and location) that uniquely identifies each component. Maintaining the baseline configuration involves creating a new baseline as the system changes over time and keeping old baselines available for possible rollback.

For software not in the direct control of the organization, this requirement stipulates a list of approved browser software, network and application protocols, and other items that must be used by a third party wanting to communicate with the organization's system..

DHS-2.6.2.3 Requirement Enhancements

1. The organization reviews and updates the baseline configuration as an integral part of system component installations.
2. The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the system.
3. The organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.

4. The organization employs a deny-all, permit-by-exception authorization policy to identify hardware and software allowed on (or allowed to access or interoperate with) organizational systems.

DHS-2.6.2.4 Rationale

This is a recognized best practice. This control extends the original DHS control to include configuration requirements for software that accesses or interoperate with the organization's systems, even when those systems are not in the direct control of the organization.

DHS-2.6.3 Configuration Change Control

DHS-2.6.3.1 Requirement

The organization:

1. Authorizes and documents changes to the system. This includes changes to the list of (registered) software (with configuration settings) that external agents may use to interact with the system.
2. Retains and reviews records of configuration-managed changes to the system
3. Audits activities associated with configuration-managed changes to the system.

DHS-2.6.3.2 Supplemental Guidance

The organization manages configuration changes to the system using an organizationally approved process (e.g., a Configuration Control Board). Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications. Configuration change control for systems includes changes to the configuration settings for the system and those IT products (e.g. operating systems, firewalls, routers) that are components of the system. Each device on the system contains a unique identifier (e.g., serial number, device name, tag number) that is referenced in the configuration management process. The organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws. The approvals to implement a change to the system include successful results from the security analysis of the change. The organization audits activities associated with configuration changes to the system.

A production system may need to be taken offline, or replicated to the extent feasible, before testing can be conducted. If a system must be taken offline for tests, tests are scheduled to occur during planned system outages whenever possible. In situations where the organization determines it is not feasible to implement the live testing of the production system, the organization documents the rationale for using a replicated system.

DHS-2.6.3.3 Requirement Enhancements

1. The organization employs automated mechanisms to:
    a. Document proposed changes to the system
    b. Notify appropriate approval authorities
    c. Highlight approvals that have not been received in a timely manner
    d. Inhibit change until necessary approvals are received
    e. Document completed changes to the system.
2. The organization tests, validates, and documents configuration changes (e.g., patches and updates) before installing them on the operational system. The organization ensures that testing does not interfere with system operations. The organization tester fully understands the organization's system security policies and procedures.

DHS-2.6.3.4 Rationale

Unrecorded and uncontrolled changes to the system may expose avoidable vulnerabilities that are not detected in a timely manner due to lack of visibility, may precipitate a system failure due to its unexpected response to a test or normal use, and in general fosters an operating environment that is unpredictable and insecure.

DHS-2.6.4 Monitoring Configuration Changes

DHS-2.6.4.1 Requirement

The organization implements a process to monitor changes to the system. This includes changes to the list of (registered) software (with configuration settings) that interoperate with the organization's system but are not in the direct control of the organization. The organization conducts security impact analyses to determine the effects of the changes.

DHS-2.6.4.2 Supplemental Guidance

Prior to change implementation, and as part of the change approval process, the organization analyzes changes to the system for potential security impacts. After the system is changed, the organization should check the security features to ensure that the features are still functioning properly and have not been subverted. Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional safeguards and countermeasures are required. Security impact analysis is an important activity in the ongoing monitoring of security controls in the system. The organization should audit activities associated with configuration changes to the system. The organization considers system security interdependencies.

DHS-2.6.4.3 Requirement Enhancements

None.

DHS-2.6.4.4 Rationale

Without active monitoring, inevitable but unexpected changes will cause the actual and perceived system configuration to diverge and defeat the purpose of the policies and procedures for managing change.

DHS-2.6.6 Configuration Settings

DHS-2.6.6.1 Requirement

The organization:

1. Establishes mandatory configuration settings for products employed within the system, and also includes requirements and mandatory configuration settings for software that interoperates with the organization's system but are not in the direct control of the organization. For example, the organization determines which web browsers, including specific versions and browser settings that Resource Owners must use to access the organization's system.
2. Configures the security settings of systems technology products to the most restrictive mode consistent with system operational requirements
3. Documents the changed configuration settings
4. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the system based on explicit operational requirements
5. Enforces the configuration settings in all components of the system
6. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

DHS-2.6.6.2 Supplemental Guidance

Configuration settings are the configurable parameters of the products that compose the system. Organizations monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

This control applies to remote assets (e.g., remote assets used to access the system, including assets owned or operated by Resource Owners or other organizations) as well as assets onsite.

DHS-2.6.6.3 Requirement Enhancements

1. The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.
2. The organization employs automated mechanisms to respond to unauthorized changes to configuration settings.

3. The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.

DHS-2.6.6.4 Rationale

Effective implementation of a configuration control policy requires that configuration settings for devices be enforced automatically within and at the entry points to the system, that the efficacy of the automatic enforcement is monitored, and that these automatic mechanisms be managed and controlled by a single, responsible party within the organization.

DHS-2.6.8 Configuration Assets

DHS-2.6.8.1 Requirement

The organization develops, documents, and maintains an inventory of the components of the system that:

1. Accurately reflects the current system, including components/devices that access or interoperate with the organization's systems but are owned or operated by other organizations or by Resource Owners.
2. Are consistent with the authorization boundary of the system
3. Are at the level of granularity deemed necessary for tracking and reporting
4. Includes defined information deemed necessary to achieve effective property accountability.

DHS-2.6.8.2 Supplemental Guidance

Before a configuration management program can operate, all configurable items should first be uniquely identified and recorded. The organization determines the appropriate level of granularity for any system component included in the inventory that is subject to management control (e.g., tracking, and reporting). The inventory of system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner, and for a networked component/device, the machine name and network address). The organization's maintenance program is responsible for configuration management tasks. Personnel performing maintenance on a system should refer to and update the configurable assets list to ensure that all system components are maintained and configured appropriately.

DHS-2.6.8.3 Requirement Enhancements

1. The organization updates the inventory of system components as an integral part of component installations and system updates.

2. The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of system components.
3. The organization employs automated mechanisms to detect the addition of unauthorized components/devices into the system (including unauthorized components/devices owned or operated by other organizations or Resource Owners that attempt to access or interoperate with the organization's system). For example, customers need to pre-register their home area network (HAN) equipment with the organization if the equipment will interact with the organization's systems.
4. The organization disables network access by such components/devices or notifies designated organizational officials.
5. The organization includes in the property accountability information for system components, the names of the individuals responsible for administering those components.

DHS-2.6.8.4 Rationale

To apply configuration requirements, to monitor conformance with requirements, and to maintain the configuration of specific devices requires knowledge of that device's existence, its location, and its custodian.

DHS-2.6.9 Addition, Removal, and Disposal of Equipment

DHS-2.6.9.1 Requirement

The organization implements policy and procedures to address the addition, removal, and disposal of all system equipment. All system assets and information are documented, identified, and tracked so that their location and function are known.

DHS-2.6.9.2 Supplemental Guidance

The organization sanitizes system media, both paper and digital, before disposal or reuse. (For further guidance, see NIST Special Publication 800-88 Guidelines for Media Sanitization.) All system media needs to be tracked, documented, and verified as sanitized. The organization periodically verifies the media sanitization process.

The organization specifies the sanitization requirements for media owned or in the control of Resource Owners or other organizations that interact with the organization's systems, as well as how the satisfaction of these requirements is to be documented and tracked. The organization provides guidance to Resource Owners on how to dispose of home equipment safely and in a manner that prevents the unauthorized or unwanted disclosure of data stored on the device.

DHS-2.6.9.3 Requirement Enhancements

None.

DHS-2.6.9.4 Rationale

Improper disposal of electronic media incurs a substantial risk of unauthorized access to sensitive data. It is therefore important that the organization discarding electronic media ensure that it has been scrubbed of information that if released could be harmful to the organization's interests. Similarly, Resource Owners should be advised how to properly dispose of media provided to them by the organization in a way that protects the Resource Owner's privacy, deters identity theft, and otherwise protects the Resource Owner's interests.

DHS-2.6.10 Factory Default Authentication Management

DHS-2.6.10.1 Requirement

The organization changes all factory default authentication credentials on system components and applications upon installation.

The organization also specifies this as a requirement for all Resource Owners' or organizations' software that is used to access or interoperate with the organization's systems.

DHS-2.6.10.2 Supplemental Guidance

Many system devices and software are shipped with factory default authentication credentials to allow for initial installation and configuration. However, factory defaults are often well known or easily discoverable. They present an obvious security risk and, therefore, should be changed prior to the device being put into service. In addition, do not embed passwords into tools, source code, scripts, aliases, or shortcuts.

DHS-2.6.10.3 Requirement Enhancements

None.

DHS-2.6.10.4 Rationale

The use of passwords and other authentication tokens that are publicly known and easily reproduced is an obvious security risk.

DHS-2.6.11 Configuration Management Plan

DHS-2.6.11.1 Requirement

The organization develops and implements a configuration management plan for the system that:

1. Addresses roles, responsibilities, and configuration management processes and procedures
2. Defines the configuration items for the system. This includes configuration requirements for software that is not in the direct control of the organization, but

rather is owned or operated by Resource Owners and other cooperating organizations, and may be used to access or interoperate with the organization's system.

3. Defines when (in the system development life cycle) the configuration items are placed under configuration management
4. Defines the means for uniquely identifying configuration items throughout the system development life cycle
5. Defines the process for managing the configuration of the controlled items. This includes providing guidance to Resource Owners and cooperating organizations on how to manage their configurations (e.g., issuing security alerts to Resource Owners about urgent security patches, providing information to Resource Owners about when and how to update their browsers, etc.).

DHS-2.6.11.2 Supplemental Guidance

Configuration items are the system items (hardware, software, firmware, and documentation). Configuration management is the management of planned configuration changes to those items. The configuration management plan satisfies the requirements in the organization's configuration management policy while being tailored to the individual system. The configuration management plan defines detailed processes and procedures for how configuration management is used to support system development life-cycle activities at the system level. It includes the steps for moving a change through the change management process; how configuration settings and configuration baselines are updated; how the system component inventory is maintained; how development, test, and operational environments are controlled; and how documents are developed, released, and updated.

DHS-2.6.11.3 Requirement Enhancements

None.

DHS-2.6.11.4 Rationale

A configuration management plan helps to ensure the integrity of the system by tracking and controlling legitimate changes as the system evolves. Because systems owned or operated by third parties may have a substantial impact on the security of the organization's system, configuration requirements for web browsers, communication protocols, and other devices that interact with the organizations should be planned, maintained, and enforced.

ASAP-2.6.12 Customer Configuration Management (New ASAP Control)

ASAP-2.6.12.1 Requirement

The Resource Owner is required to satisfy the configuration requirements specified in the organization's terms of use policy for all Resource Owner-managed software that is used

to access or interoperate with the organization's systems. In particular, with respect to software used to access the organization's systems, the Resource Owner shall:

Read the organization's terms of use policy.

1. Use only web browsers (versions and configurations) designated as acceptable by the organization in the organization's terms of use policy. Only such software types, versions, and configurations settings as defined in the organization's terms of use policy may be used to access the organization's systems.
2. Keep systems and applications up to date with the latest revisions and security patches.
3. Regularly run virus and spyware scanners with up-to-date virus and spyware signatures.
4. Change all factory default passwords on Resource Owner-managed hardware and software.
5. Sanitize all storage media before disposing of Resource Owner-owned equipment.

ASAP-2.6.12.2 Supplemental Guidance

None.

ASAP-2.6.12.3 Requirement Enhancements

None.

ASAP-2.6.12.4 Rationale

Because resource owners are included in the organization's configuration management plan, it is imperative that they be informed of configuration requirements dictated by that plan, be given information and tools sufficient to implement those requirements, and understand that compliance with configuration requirements is a prerequisite for access to the organization's systems.

DHS-2.9 Information and Document Management

Information and document management is generally a part of the organization's records retention and document management system. Digital and hardcopy information associated with the development and execution of an information system is important and sensitive and must be managed. System design, operations data and procedures, risk analyses, business impact studies, risk tolerance profiles, etc., contain sensitive company information and must to be protected. Security measures, philosophy, and implementation strategies are other examples. In addition, business conditions change and require updated analyses and studies. Care is given to protect this information and verify that the appropriate versions are retained. Inherent in this is an information

classification system that allows information assets to receive the appropriate level of protection.

The following are the controls for Information and Document Management that must be supported and enforced by the organization and its systems for providing data to third parties.

DHS-2.9.1 Information and Document Management Policy and Procedures

DHS-2.9.1.1 Requirement

The organization shall develop, disseminate, and periodically review and update:

1. A formal, documented, information and document management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
2. Formal, documented procedures to facilitate the implementation of the information and document management policy and associated system maintenance controls.

DHS-2.9.1.2 Supplemental Guidance

The organization shall ensure that the information and document management policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The information and document management policy can be included as part of the general information security policy for the organization. System information and document management procedures can be developed for the security program in general and for a particular system component when required.

DHS-2.9.1.3 Requirement Enhancements

Document management policies must include conditions under which parties external to the organization may access its data, what types of data and how frequently it may be accessed, rules governing the redistribution and retention of data by the third party, and processes for auditing and enforcing these rules and conditions.

DHS-2.9.1.4 Rationale

Gaps and inconsistencies in defenses may occur if Information and Document Management Policy and Procedures are not developed, documented, and disseminated within the Resource Custodian and Third Party organizations. Periodic reviews will ensure that the policies and procedures evolve to meet any system, technology, or business requirement changes.

As Resource Owners in many cases will be individual residential electricity consumers, Resource Custodians and Third Parties should provide guidance to Resource Owners to promote end-to-end security.

DHS-2.9.2 Information and Document Retention

DHS-2.9.2.1 Requirement

The organization shall manage system-related data, including establishing retention policies and procedures for both electronic and paper data and manage access to the data based on formally assigned roles and responsibilities.

DHS-2.9.2.2 Supplemental Guidance

The organization shall develop policies and procedures detailing the retention of company information. These procedures address retention/destruction issues for all applicable information media. Any legal or regulatory requirements are considered when developing these policies and procedures.

DHS-2.9.2.3 Requirement Enhancements

The organization shall perform legal reviews of the retention policies to ensure compliance with all applicable laws and regulations. These policies must also govern retention of data by third parties and procedures for auditing and enforcing compliance of those third parties with the terms of use.

DHS-2.9.2.4 Rationale

Gaps and inconsistencies in defenses may occur if Information and Document Retention policies are not developed, documented, and disseminated within the Resource Custodian and Third Party organizations. Periodic reviews will ensure that the policies and procedures evolve to meet any system, technology, or business requirement changes.

As Resource Owners in many cases will be individual residential electricity consumers, Resource Custodians and Third Parties should provide guidance to Resource Owners to promote end-to-end security.

DHS-2.9.3 Information Handling

DHS-2.9.3.1 Requirement

Organization implemented policies and procedures detailing the handling of information shall be developed and periodically reviewed and updated.

DHS-2.9.3.2 Supplemental Guidance

Written policies and procedures detail access, sharing, copying, transmittal, distribution, and disposal or destruction of documents and information. These policies or procedures include the periodic review of all managed documents and information to ensure it is

properly handled. The organization must protect information against unauthorized access, misuse, or corruption during transportation or transmission. The organization distributes or shares information on a need-to-know basis and considers legal and regulatory requirements when developing these policies and procedures.

DHS-2.9.3.3 Requirement Enhancements

Rules for sharing and redistribution of data by third parties must be included in these policies and procedures along with processes for auditing and enforcement of these rules.

DHS-2.9.3.4 Rationale

Gaps and inconsistencies in defenses may occur if appropriate Information Handling procedures are not developed, documented, and disseminated within the Resource Custodian and Third Party organizations. Periodic reviews will ensure that the policies and procedures evolve to meet any system, technology, or business requirement changes. Proper Information Handling should consider risks associated with social engineering.

As Resource Owners in many cases will be individual residential electricity consumers, Resource Custodians and Third Parties should provide guidance to Resource Owners to promote end-to-end security.

DHS-2.9.8 Information and Document Destruction

DHS-2.9.8.1 Requirement

The organization shall develop policies and procedures detailing the destruction of written and electronic records, equipment, and other media without compromising the confidentiality of the data.

DHS-2.9.8.2 Supplemental Guidance

The organization must develop policies and procedures detailing the destruction and disposal of written and electronic records, equipment, and other media in the overall information and document management policy. This also includes the method of disposal such as shredding of paper records, erasing of disks or other electronic media, or physical destruction. All legal or regulatory requirements must be considered when developing these policies and procedures.

DHS-2.9.8.3 Requirement Enhancements

Policies and procedures must also address the destruction of documents and information by third parties, to describe acceptable mechanisms for destruction and procedures for assuring compliance with the organization's policies.

DHS-2.9.8.4 Rationale

Gaps and inconsistencies in defenses may occur if appropriate Information and Document Destruction is not developed, documented, and disseminated within the

Resource Custodian and Third Party organizations. Periodic reviews will ensure that the policies and procedures evolve to meet any system, technology, or business requirement changes. Proper Information and Document Destruction should consider risks associated with social engineering.

As Resource Owners in many cases will be individual residential electricity consumers, Resource Custodians and Third Parties should provide guidance to Resource Owners to promote end-to-end security.

DHS-2.9.9 Information and Document Management Review

DHS-2.9.9.1 Requirement

The organization shall perform periodic reviews of compliance with the organization's information and document security management policy to ensure compliance with any laws and regulatory requirements.

DHS-2.9.9.2 Supplemental Guidance

The organization must periodically review compliance in the information and document management security policy. The compliance review procedure must consider all legal and regulatory documentation requirements applicable to the organization.

DHS-2.9.9.3 Requirement Enhancements

Third parties are subject to audit for compliance in accordance with policies and procedures governing the sharing, retention, and destruction of data provided to the third party by the organization.

DHS-2.9.9.4 Rationale

Gaps and inconsistencies in defenses may occur if appropriate Information and Document Management Review procedures are not developed, documented, and disseminated within the Resource Custodian and Third Party organizations. Periodic reviews will ensure that the policies and procedures evolve to meet any system, technology, or business requirement changes.

DHS-2.10 System Development and Maintenance

Security is most effective when it is designed into the system and sustained, through effective maintenance, throughout the life cycle of the system and through all future configurations. Maintenance activities must encompass appropriate policies and procedures for performing routine and preventive maintenance on the components of a system.

DHS-2.10.4 Backup and Recovery

DHS-2.10.4.1 Requirement

The organization shall make and secure backups of critical data for use if the operational copies are corrupted or destroyed.

DHS-2.10.4.2 Supplemental Guidance

Data may be compromised due to an incident or disaster. Therefore, copies of essential data need to be created, updated regularly, and stored in a secure environment so that it can be used to restore normal operations following an incident.

DHS-2.10.4.3 Requirement Enhancements

The organization must periodically test and validate backup and recovery procedures, data, and media.

DHS-2.10.4.4 Rationale

Gaps and inconsistencies in defenses may occur if appropriate Backup and Recovery procedures are not established, tested, and implemented rigorously within the Resource Custodian and Third Party organizations. Periodic reviews will ensure that the policies and procedures evolve to meet any system, technology, or business requirement changes.

DHS-2.11 Security Awareness and Training

Physical and cyber security awareness (which includes privacy concerns) is a critical part of information and control system incident prevention, particularly with regard to social engineering threats. Social engineering is a technique used to manipulate individuals into giving away confidential security-relevant information such as passwords or revealing sensitive Resource Owner data, such as personally identifiable information (PII) that, for example, may uniquely associate detailed records of electricity usage with specific Resource Owners. Inadvertently disclosed security-relevant information can be used to compromise otherwise secure systems. Revealing PII to an unauthorized person or entity is a violation of Resource Owner privacy that can bring harm to the Resource Owner in a variety of ways and can also damage the reputation of the organization that had been entrusted with the care of that data.

Implementing a system cyber security and privacy awareness training controls program may change the way personnel access computer programs and applications, so organizations need to design effective cyber security and privacy awareness training programs based on individuals' roles and responsibilities. Communication vehicles need to be developed to help employees understand why new access and control methods are required and how they can reduce risks and impacts to the organization. Training programs also need to demonstrate management's commitment to information and control system security programs and to the protection of Resource Owner privacy. Feedback from staff can be valuable for refining the security program. In addition, educational materials (e.g., documents, videos, web-based training) should be provided to

Resource Owners to help them understand the steps they need to take to protect their own privacy and security while gaining the benefits of third party data access smart grid technology and services.

Following are the controls for awareness and training that need to be supported and implemented by the organization to protect not only the systems involved in third party data access, but also the security and privacy of the associated business and Resource Owner data.

DHS-2.11.1 Security Awareness and Training Policy and Procedures

DHS-2.11.1.1 Requirement

The organization develops, disseminates, and periodically reviews and updates:

1. A formal, documented, security awareness and training policy (which specifically includes the protection of Resource Owner privacy) that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
2. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

DHS-2.11.1.2 Supplemental Guidance

The organization ensures the security awareness and training policy and procedures are consistent with applicable federal and state laws, directives, policies, regulations, standards, and guidance. These security awareness and training policy and procedures specifically include the protection of Resource Owner privacy as one of the primary objectives. The security awareness and training policy can be included as part of the general information security and privacy policy for the organization. Security awareness and training procedures can be developed for the security program in general and for particular security and privacy concerns (e.g., associated with third party data access smart grid service offerings) when required.

As Resource Owners in many cases will be individual residential electricity consumers, Resource Custodians and Third Parties should include guidance to Resource owners in their Security Awareness and Training Policy and Procedures to promote end-to-end security.

DHS-2.11.1.3 Requirement Enhancements

None.

DHS- 2.11.1.4 Rationale

Gaps and inconsistencies in the organizational security program may occur if Security Training and Awareness Policies and Procedures are not developed, implemented, and

tested. Periodic reviews will ensure that the policies and procedures evolve to meet any system, technology, or business requirement changes.

DHS- 2.11.2 Security Awareness

DHS- 2.11.2.1 Requirement

The organization provides basic security awareness training (that includes privacy issues and concerns) to all system users (including managers, senior executives, and contractors) before authorizing access to the system, when required by system changes, and at least annually thereafter. The effectiveness of security awareness training, at the organization level, needs to be reviewed at least once a year at a minimum with the objective of continual improvement.

DHS- 2.11.2.2 Supplemental Guidance

The organization determines the content of security awareness training and security awareness techniques based on the specific requirements of the organization and the systems to which personnel have authorized access. Security and privacy awareness techniques can include displaying posters, offering security-messaged items, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting security awareness events. The security awareness training program is consistent with the requirements contained in Code of Federal Regulations (CFR) Part 5 Subpart C (5 CFR 930.301).

DHS- 2.11.2.3 Requirement Enhancements

1. All system design and procedure changes need to be reviewed by the organization for inclusion in the organization security awareness training.
2. The organization includes practical exercises in security awareness training that simulate actual cyber attacks, unauthorized physical access, and social engineering attempts.

DHS- 2.11.2.4 Rationale

Organizations need buy-in from all users for a security program to be affective. Awareness is essential for users to understand and accept the need for the specified security policies, procedures, and controls.

DHS- 2.11.3 Security Training

DHS- 2.11.3.1 Requirement

The organization:

1. Defines and documents system security roles and responsibilities, including the protection of Resource Owner privacy, throughout the system development life cycle

2. Identifies individuals having system security roles and responsibilities
3. Provides security-related technical training: (a) before authorizing access to the system or performing assigned duties, (b) when required by system changes, and (c) on an organization-defined frequency thereafter.

DHS- 2.11.3.2 Supplemental Guidance

The organization determines the content of security training based on assigned roles and responsibilities and the specific requirements of the organization and the systems to which personnel have authorized access. In addition, the organization provides system managers, system and network administrators, and other personnel having access to system-level software, security-related technical training to perform their assigned duties. The organization's security training program is consistent with the requirements contained in CFR Part 5 Subpart C (5 CFR 930.301).

DHS- 2.11.3.3 Requirement Enhancements

None.

DHS- 2.11.3.4 Rationale

Gaps or inconsistencies in the organizations security posture may result from unclear or undefined security roles and responsibilities or lack of adequate technical training for key personnel.

DHS- 2.11.4 Security Training Records

DHS- 2.11.4.1 Requirement

The organization documents, maintains, and monitors each user's security and privacy training activities on an individual basis, including basic security awareness training and specific information and control system security training in accordance with the organization's records retention policy.

DHS- 2.11.4.2 Supplemental Guidance

The organization maintains a record of training requirements for each user in accordance with the provisions of the organization training and records retention policy.

DHS- 2.11.4.3 Requirement Enhancements

None.

DHS- 2.11.4.4 Rationale

Without adequate training records, organizations may not be able to adequately track personnel that are not be allowed access to the third party data access system and thus undermine the effectiveness of the security awareness and training program.

DHS- 2.11.5 Contact with Security/Privacy Groups and Associations

DHS- 2.11.5.1 Requirement

The organization establishes and maintains contact with security and privacy groups and associations to stay up to date with the latest recommended security and privacy practices, techniques, and technologies and to share current information on threats, vulnerabilities, and incidents.

DHS- 2.11.5.2 Supplemental Guidance

Security and privacy groups and associations can include special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security and privacy professionals in similar organizations. The groups and associations selected are consistent with the organization's mission/business requirements. Information sharing activities regarding threats, vulnerabilities, and incidents related to systems are consistent with applicable laws, directives, policies, regulations, standards, and guidance.

DHS- 2.11.5.3 Requirement Enhancements

None.

DHS- 2.11.5.4 Rationale

Due to the specialized nature of third party data access systems and components, it is essential for the organization to interact with groups well versed in the relevant technology as well as those well versed in the operational and business aspects of the system.

Due to the large amounts of Resource Owner oriented data, it is essential for the organization to solicit feedback and input from groups and associations well versed in consumer privacy issues.

DHS- 2.11.6 Security Responsibility Testing

DHS- 2.11.6.1 Requirement

The organization documents and tests the knowledge of personnel on security policies and procedures based on their roles and responsibilities to ensure that they understand their responsibilities in securing not only the control systems, but also in protecting the security and privacy of the associated business and Resource Owner data.

DHS- 2.11.6.2 Supplemental Guidance

The organization maintains a list of security and privacy responsibilities for each user. These need to be used to test each user in accordance with the provisions of the organization training policy. Users must be notified when their testing is scheduled, informed as to how it will be conducted, and notified of the results. The security

responsibility testing needs to be conducted at least annually and/or as warranted by technology/procedural changes.

DHS- 2.11.6.3 Requirement Enhancements

None.

DHS- 2.11.6.4 Rationale

Testing is essential in measuring the effectiveness of the organizations security awareness and training program.

ASAP-2.11.7 Resource Owner Awareness and Education (New ASAP Control)

ASAP-2.11.7.1 Requirement

The organization provides its Resource Owners with educational materials that (a) raise awareness about security and privacy risks associated with the Resource Owners' use of third party data access use of smart grid technology and services, (b) summarize the steps that the organization is taking to reduce those risks, and (c) describe the steps that Resource Owners can take to help reduce their own risk.

ASAP-2.11.7.2 Supplemental Guidance

Educational materials may be in the form of hardcopy or electronic documents, videos, or web-based training materials, including links to educational and training material from other organizations such as public interest groups (e.g., privacy advocacy organizations). The objective of these education materials is to improve the Resource Owners' understanding of the security and privacy risks associated with the Resource Owners' use of third party data access grid services and to provide actionable guidance on the steps a Resource Owner can take to help reduce those risks. For example, the materials should improve the Resource Owners' ability to make informed decisions about the security and privacy options available to them under the organization's security and privacy policies, in the context of third party data access smart grid services being offered. The materials should provide sufficient information to encourage and enable Resource Owners to follow good security practices (e.g., changing default passwords on home equipment, choosing strong passwords), and to become more resistant to social engineering attacks in the form of phishing e-mails, phishing phone calls, and other scams.

ASAP-2.11.7.3 Requirement Enhancements

The effectiveness of the educational materials should be evaluated and reviewed at least annually, with the objective of continual improvement. In particular, the educational materials need to keep pace with the organization's modifications to third party data access introduction of new smart grid services and the lessons learned from relevant security and privacy incidents, vulnerabilities, and threats. The organization should also provide its Resource Owners with timely alerts about newly emerging threats relevant to

the Resource Owners' use of smart grid (or value-added) services. For example, an alert might detail the specific characteristics of a currently active widespread phishing attack targeted at users of third party data access particular smart grid service and provide guidance to Resource Owners on how to avoid falling victim to the attack.

ASAP-2.11.7.4 Rationale

Resource Owner awareness and good practice is a crucial link in the security and privacy chain.

DHS-2.14 System and Information Integrity

Maintaining a third party data access Party Data Access system, including information integrity, increases assurance that sensitive data have neither been modified nor deleted in an unauthorized or undetected manner. The security controls described under the system and information integrity family provide policy and procedure for identifying, reporting, and correcting third party data access Party Data Access system flaws. In general, controls identified in this section directly apply to the Resource Custodian (referred to as "The organization") and indirectly extend to the Resource Owner and Third Party when interacting with the Resource Custodian.

Controls exist for malicious code detection, spam protection, and tools and techniques. Also provided are controls for receiving security alerts and advisories and the verification of security functions on the third party data access Party Data Access system. In addition, controls within this family detect and protect against unauthorized changes to software and data; restrict data input and output; check the accuracy, completeness, and validity of data; and handle error conditions.

DHS-2.14.2 Flaw Remediation

DHS-2.14.2.1 Requirement

The organization:

1. Identifies, reports, and corrects system flaws
2. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational systems before installation
3. Incorporates flaw remediation into the organizational configuration management process as an emergency change.

DHS-2.14.2.2 Supplemental Guidance

The organization identifies third party data access systems containing software affected by recently announced flaws (and potential vulnerabilities resulting from those flaws). The organization (or the software developer/vendor for software developed and maintained by a vendor/contractor) promptly evaluates newly released security-relevant

patches, service packs, and hot fixes and tests them for effectiveness and potential impacts on the organization's third party data access system before installation. Flaws discovered during security assessments, continual monitoring, or under incident response activities also need to be addressed expeditiously. It is generally not recommended to shut down and restart third party data access system components when an anomaly is identified. It is also not recommended to automatically install updates to third party data access systems without close monitoring and supervision.

Organizations should develop, document, and review plans for installation of updates including system backups and steps necessary to back out of the update process and revert to the pre-update state if necessary.

DHS-2.14.2.3 Requirement Enhancements

1. The organization centrally manages the flaw remediation process.
2. The organization employs automated mechanisms to periodically and on demand determine the state of system components with regard to flaw remediation.
3. The organization measures the time between flaw identification and flaw remediation, comparing with organization-defined benchmarks.
4. The organization employs centralized patch management tools to facilitate flaw remediation to organization-defined third party data access system components.
5. The flaw remediation processes must not degrade the operational performance of the third party data access Party Data Access system.

DHS-2.14.2.4 Rationale

It is anticipated that a majority of third party data access systems will utilize use the Internet as the main communications vehicle. Flaw remediation and security patch management will reduce or eliminate the potential for exploitation and involve considerably less time and effort than responding after exploitation has occurred.

DHS-2.14.3 Malicious Code Protection

DHS-2.14.3.1 Requirement

The organization:

1. Employs malicious code protection mechanisms at system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: (a) transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means or (b) inserted through the exploitation of system vulnerabilities
2. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures

3. Configures malicious code protection mechanisms to: (a) perform periodic scans of the system on an organization-defined frequency and real-time scans of files from external sources as the files are downloaded, opened, or executed and (b) disinfect and quarantine infected files
4. Considers using malicious code protection software products from multiple vendors as part of defense-in-depth
5. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

DHS-2.14.3.2 Supplemental Guidance

The organization employs malicious code protection mechanisms at critical third party data access system entry and exit points (e.g., firewalls, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the malicious code protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware). The organization updates malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures. The organization considers using malicious code protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). The organization also considers the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the third party data access system.

Updates are scheduled to occur during planned third party data access system outages. The organization considers third party data access system vendor recommendations for malicious code protection. To reduce malicious code, organizations remove the functions and services that should not be employed on the third party data access system (e.g., VoIP, Instant Messaging, file transfer protocol, HTTP, electronic mail, file sharing).

DHS-2.14.3.3 Requirement Enhancements

1. The organization centrally manages malicious code protection mechanisms.
2. The system prevents users from circumventing host-based malicious code protection capabilities.
3. The system updates malicious code protection mechanisms only when directed by a privileged user.
4. The organization does not allow users to introduce removable media into the system.
5. The system implements malicious code protection mechanisms to identify data containing malicious code and responds accordingly (i.e., block, quarantine, send alert to administrator) when the system encounters data not explicitly allowed by the security policy. The use of mechanisms to centrally manage malicious code

protection shall not interfere with the reliable operation of the third party data access system.

6. All signature files and definitions for malicious code detection mechanisms used within the third party data access system shall be updated automatically from a centralized managed trusted source.
7. Centralized configuration management and change control shall be employed for all third party data access system assets.
8. Periodic and automatic auditing/verification of configuration (programming parameters, firmware and rev level, etc.) shall be performed for all third party data access system assets.
9. All detection of and actions taken within the third party data access system to respond to malicious code shall be logged to a centralized repository.
10. Scanning of incoming and outgoing network traffic for viruses, spyware, or malware shall be employed within the third party data access system.
11. Dynamic packet filtering shall be employed at external interface points.
12. The transfer of executable files shall be prohibited through the external interface points.
13. All components of the third party data access system or any device connected to the network segments within the boundaries of the third party data access system shall employ host hardening, including patch application and security-minded configurations of the operating system (OS), browsers, and other network-aware software.
14. All firmware/software shall be scanned for malicious code prior to loading on any component of the third party data access system or device connected to the AMI network.
15. The authenticity and integrity of all firmware/software shall be verified prior to loading on any component of the third arty data access system or any device connected to the network segments within the boundaries of the third party data access system.
16. All devices shall be verified to have the proper software revisions and patches prior to being allowed full operation within the third party data access system.
17. All components of the third party data access system shall employ anti-virus software.
18. Maintenance and monitoring tools which are not permanently connected to the third party data access system network shall have additional control applied as follows:

a. Security updates from the manufacturer of the appropriate operating system, and/or application software, shall be kept current (e.g., patched and updated) on all field tools.

b. Maintenance and monitoring tools shall employ firewall software or hardware shall to aid in the prevention of malicious code attacks/infections.

c. Maintenance and monitoring tools shall employ host hardening, including patch application and security-minded configurations of the operating system (OS), browsers, and other network-aware software.

d. Maintenance and monitoring tools shall utilize anti-virus, anti-spam, and anti-spyware software.

e. Maintenance and monitoring tools shall scan removable media devices for malicious code before accessing any data on the media.

f. Maintenance and monitoring tools shall scan email attachments and shared files of unknown integrity for malicious code before they are opened or accessed.

g. Requirement Enhancement(s):

    i. The maintenance and monitoring tools shall use a restricted operating system which only allows execution of known and signed code/applications.

DHS-2.14.3.4 Rationale

It is anticipated that a majority of the external interfaces for third party data access applications will be Internet facing web based applications and failure to adequately protect these system from impacts associated with malicious code exposes the organization to significant risks.

Additionally consideration needs to be given to the fact that Resource Owners in many cases will be individual residential electricity consumers. Without adequate controls in place, Resource Custodians and Third Parties cannot protect against these users, deliberately or not, transmitting malicious code into the third party data access system. In a similar fashion, without adequate controls in place, Resource Custodians and Third Parties cannot protect against transmitting malicious code to the Resource Owners.

DHS-2.14.4 System Monitoring Tools and Techniques

DHS-2.14.4.1 Requirement

The organization:

1. Monitors events on the system
2. Detects system attacks

3. Identifies unauthorized use of the system
4. Deploys monitoring devices (a) strategically within the system to collect organization-determined essential information and (b) at ad hoc locations within the system to track specific types of transactions of interest to the organization
5. Heightens the level of system monitoring activity whenever an indication of increased risk exists to organizational operations and assets, individuals, other organizations, or the nation based on law enforcement information, intelligence information, or other credible sources of information
6. Consults legal counsel with regard to system monitoring activities.

DHS-2.14.4.2 Supplemental Guidance

Third party data access system monitoring capability can be achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, log monitoring software, network monitoring software, and network forensic analysis tools). Monitoring devices can be strategically deployed within the third party data access system (e.g., at selected perimeter locations and/or near server farms supporting critical applications) to collect essential information. Monitoring devices also can be deployed at ad hoc locations within the system to track specific transactions. In addition, these devices can be used to track the impact of security changes to the third party data access system.

Including the most information in log files is essential and in general, all logs from third party data access system components should answer the five basic questions of Who, What, Where, When, and How. When determining the actions of reading, writing, deleting, and modification of data, it should be possible to determine what process, who owns it, when it was initiated, where the action occurred, and why the process ran. Additionally, all administrative, authentication, authorization, and communication events associated with any third party data access system component should be logged and reported. The granularity of the information collected can be determined by the organization based on its monitoring objectives and the capability of the third party data access system to support such activities. An example of a specific type of transaction of interest to the organization with regard to monitoring is HTTP traffic that bypasses organizational HTTP proxies, when use of such proxies is required. Organizations need to consult with appropriate legal counsel with regard to all system monitoring activities.

The level of system monitoring activity is heightened by organizations whenever an indication of increased risk exists to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

DHS-2.14.4.3 Requirement Enhancements

1. Logs generated by third party data access system components shall conform to all applicable recommendations outlined in NIST SP800-92, Guide to Computer Security Log Management.

2. The third party data access system component shall support standard syslog format (RFC 3164).The organization interconnects and configures individual intrusion detection tools into a system wide intrusion detection system using common protocols.
3. The third party data access system component shall provide a mechanism by which missing logs and log entries are detected.
4. The organization employs automated tools to support near real-time analysis of events.
5. The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.
6. The third party data access system monitors inbound and outbound communications for unusual, anomalous, or unauthorized activities or conditions. Anomalous/unusual/unauthorized activities or conditions include the presence of malicious code, the unauthorized export of information, or signaling to an external third party data access system.
7. The third party data access system provides a real-time alert when indications of compromise or potential compromise occur.
8. The system prevents users from circumventing host-based intrusion detection and prevention capabilities.
9. The system notifies a defined list of incident response personnel of suspicious events and takes a defined list of least-disruptive actions to terminate suspicious events. Note: The least-disruptive actions may include initiating request for human response.
10. The organization protects information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion.
11. The organization tests/exercises intrusion monitoring tools on a defined time-period. Note: The frequency of testing/exercises is dependent on the type and method of deployment of the intrusion monitoring tools.
12. The organization makes provisions so that encrypted traffic is visible to system monitoring tools. Note: The enhancement recognizes the need to balance encrypting traffic versus the need to have insight into that traffic from a monitoring perspective. For some organizations, the need to ensure the confidentiality of traffic is paramount, for others the mission assurance concerns are greater.
13. The system analyzes outbound communications traffic at the external boundary of the system (i.e., system perimeter) and, as deemed necessary, at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies. Note: Anomalies within the system include large file transfers, long-time persistent

connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.

14. The third party data access system component must be capable of storing a sufficient number of security events in the components buffer to support the system-wide monitoring function.
15. The use of monitoring tools and techniques must not adversely impact the operational performance of the third party data access system.

DHS-2.14.4.4 Rationale

System monitoring is essential for the detection of system error conditions or unauthorized activity (malicious or otherwise) and initiating the organizations incident response plan to mitigate any potential impact of the event. Data collected by the monitoring components (host based and standalone) allows for proper forensics to take place after the event.

DHS-2.14.11 Error Handling

DHS-2.14.11.1 Requirement

The third party data access system:

1. Identifies error conditions
2. Generates error messages or alerts that provide information necessary for corrective actions without revealing potentially harmful information that could be exploited by adversaries
3. Reveals error messages only to authorized personnel
4. Prohibits inclusion of sensitive information in error logs or associated administrative messages.

DHS-2.14.11.2 Supplemental Guidance

The structure and content of error messages need to be carefully considered by the organization. Error messages generated by the third party data access system need to provide timely and useful information without providing potentially harmful information that could be exploited by adversaries. System error messages are revealed only to authorized personnel (e.g., systems administrators, maintenance personnel). Sensitive information (e.g., account numbers, passwords, and personnel ID numbers) is not to be listed in error logs or associated administrative messages. The extent the third party data access system is able to identify and handle an error condition is guided by organizational policy and operational requirements.

Risks associated with improper error handling are not limited to those which are transparent to the system operation. Third party data access system components should not be susceptible to security problems caused by improper error handling, such as:

- Fail-open security check – The component should assume no access until proven otherwise. All security mechanisms should deny access until specifically granted, not grant access until denied, which is a common reason why fail open errors occur.
- Impacts to component resources - Errors that can cause the component to crash or consume significant resources, effectively denying or reducing service to legitimate users.

DHS-2.14.11.3 Requirement Enhancements

None.

DHS-2.14.11.4 Rationale

Detailed records of software failures (e.g., core dumps, names of missing link libraries, and other specific, technical information) are frequently used to find and exploit security holes. Restricting access to this type of information is therefore an important security practice. Secure coding practices that help prevent security breaches following a software error are a widely documented best practice that should be followed by organizations developing software for third party data access components.

DHS-2.14.12 Information Output Handling and Retention

DHS-2.14.12.1 Requirement

The organization handles and retains output from the third party data access system in accordance with applicable laws, regulations, standards, and organizational policy as well as operational requirements of the third party data access process.

DHS-2.14.12.2 Supplemental Guidance

Output from the third party data access system represents a business, and sometimes contractual, relationship between two or more parties. Output from the third party data access system should be handled as to ensure non-repudiation by all involved parties. For the purpose of this control, output is defined as one of the following:

- Data set
- Shared resource key

In conjunction with output handling and retention, another issue is that of the security of storage media and how well electronic documents are protected for both current and future use. The output retention requirement means that current technology must be able to support what was stored at a point in the past. Due to rapid changes in technology, some media currently in use may become outdated in the next three or five years.

DHS-2.14.12.3 Requirement Enhancements

None.

DHS-2.14.12.4 Rationale

Without proper handling and retention controls, output from the third party data access system is susceptible to unauthorized manipulation or deletion.

DHS-2.15 Access Control

The focus of access control is ensuring that resources are only accessed by the appropriate personnel and that personnel are correctly identified. The first step in access control is creating access control lists with access privileges for personnel. The next step is to implement security mechanisms to enforce the access control lists. Mechanisms also need to be placed to monitor access activities for inappropriate activity. The access control lists need to be managed through adding, altering, and removing access rights as necessary.

Identification and authentication is the process of verifying the identity of a user, process, or device, as a prerequisite for granting access to data. Identification could be a password, a token, or a fingerprint. Authentication is the challenge process to prove (validate) the identification provided. An example would be using a fingerprint (identification) to access a computer via a biometric device (authentication). The biometric device authenticates the identity of the fingerprint.

DHS-2.15.8 Separation of Duties

DHS-2.15.8.1 Requirement

The organization:

1. Establishes division of responsibilities and separates duties of individuals as necessary to eliminate conflicts of interest.
2. The organization shall implement separation of duties through assigned system access authorizations. In particular, responsibility for auditing of information, entry of information into the system, and distribution of information to third parties shall be assigned to logically separate entities.

DHS-2.15.8.2 Supplemental Guidance

Separation of duties prevents users from having the system access necessary to perform malevolent activity without collusion. Examples of separation of duties include (1) mission functions and distinct system support functions are divided among different individuals and roles, (2) different individuals perform system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security), and (3) security personnel who administer access control functions do not administer audit functions.

The system should enforce separation of duties between users having system access in order to prevent malevolent activity without collusion. Points of enforcement are (1)

system support functions performed by different individuals (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security), and (2) access control functions are not administered by security personnel who also execute audit functions.

DHS-2.15.8.3 Requirement Enhancements

None.

DHS-2.15.8.4 Rationale

By having separate users responsible for logically distinct tasks, the opportunity for any single individual to cause harm is limited.

By having separate users responsible for data entry and maintenance, data distribution, and auditing, at least two parties are needed to succeed in covertly modifying data (data entry and auditing); to succeed in falsifying or manufacturing data (data entry and auditing); or to succeed in wrongly discrediting information (any pair).

DHS-2.15.9 Least Privilege

DHS-2.15.9.1 Requirement

The organization employs the concept of least privilege, limiting authorized access for users (and processes acting on behalf of users) as necessary, to accomplish assigned tasks.

DHS-2.15.9.2 Supplemental Guidance

The organization employs the concept of least privilege for specific duties and system functions (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.

DHS-2.15.9.3 Requirement Enhancements

1. The organization explicitly authorizes access to organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information. Note: Explicitly authorized personnel include security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.
2. The organization requires that users of system accounts with access to organization-defined lists of security functions or security-relevant information, use non-privileged accounts when accessing other system functions, and if feasible, audits any use of privileged accounts for such functions.

DHS-2.15.9.4 Rationale

Opportunity to violate policies for accessing data is minimized if individuals are restricted to just those activities required to perform their function within the organization.

DHS-2.16 Audit and Accountability

Periodic audits and logging of the data management system must be implemented to validate that the security mechanisms present during system validation testing are still installed and operating correctly. These security audits review and examine a system's records and activities to determine the adequacy of system security controls and to ensure compliance with established security policy and procedures. Audits also are used to detect breaches in security services through examination of system logs. Logging is necessary for anomaly detection, as well as forensic analysis.

DHS-2.16.1 Audit and Accountability Policy and Procedures

DHS-2.16.1.1 Requirement

The organization shall develop, disseminate, and periodically review and update:

1. A formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
2. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

DHS-2.16.1.2 Supplemental Guidance

The organization must ensure that the audit and accountability policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The audit and accountability policy can be included as part of the general security policy for the organization. Procedures shall be developed for the security program in general and for a particular data management system when required.

DHS-2.16.1.3 Requirement Enhancements

Where third parties are restricted in regards to redistribution and sharing of data provided by the organization, the organization must establish policies and procedures sufficient to ensure that data provided to it is adequately protected and not subject to access in violation of the terms of use for that data.

DHS-2.16.1.4 Rationale

Gaps and inconsistencies in defenses may go undetected if appropriate Audit and Accountability Policies and Procedures are not developed, documented, and disseminated within the Resource Custodian and Third Party organizations. Periodic reviews will

ensure that the policies and procedures evolve to meet any system, technology, or business requirement changes.

DHS-2.16.2 Auditable Events

DHS-2.16.2.1 Requirement

The organization:

1. Determines, based on a risk assessment in conjunction with mission/business needs, which system-related events require auditing (e.g., an organization-defined list of auditable events and frequency of [or situation requiring] auditing for each identified auditable event)
2. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events
3. Ensures that auditable events (e.g. logs, records) are adequate to support after-the-fact investigations of security incidents
4. Adjusts, as necessary, the events to be audited within the system based on current threat information and ongoing assessments of risk.

DHS-2.16.2.2 Supplemental Guidance

The purpose of this control is for the organization to identify events that need to be auditable as significant and relevant to the security of the system. Audit records shall be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level and type of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events.

DHS-2.16.2.3 Requirement Enhancements

1. The organization must review and update the list of organization-defined auditable events on an organization-defined frequency.
2. The organization must include execution of privileged functions in the list of events to be audited by the system.
3. The organization must include in its list of auditable events conditions under which a third party that has been supplied with data will be subject to an audit.

DHS-2.16.2.4 Rationale

Gaps and inconsistencies in defenses may go undetected if appropriate guidelines for observable events are not developed, tested, and implemented within the Resource Custodian and Third Party organizations. Without appropriate standards and procedures,

may lead to an organization may become overwhelmed with too much information or lacking enough information to support proper anomaly detection and forensics.

DHS-2.16.6 Audit Monitoring, Analysis, and Reporting

DHS-2.16.6.1 Requirement

The organization must:

1. Review and analyze system audit records on an organization-defined frequency for indications of inappropriate or unusual activity and reports findings to designated organizational officials
2. Adjust the level of audit review, analysis, and reporting within the system when a change in risk exists to organizational operations, organizational assets, individuals, other organizations, or the nation based on law enforcement information, intelligence information, or other credible sources of information.

DHS-2.16.6.2 Supplemental Guidance

Organizations shall increase the level of audit monitoring and analysis activity whenever an indication of increased risk exists to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information. Audit records must be monitored regularly for inappropriate activities in accordance with organizational procedures. Audit reports need to be provided to those responsible for cyber security.

DHS-2.16.6.3 Requirement Enhancements

1. The system shall employ mechanisms to integrate audit review, analysis, and reporting into organizational processes for investigation and response to suspicious activities.
2. The organization shall analyze and correlate audit records across different repositories to gain organization-wide situational understanding.
3. The system shall employ automated mechanisms to centralize audit review and analysis of audit records from multiple components within the system. Note: An example of an automated mechanism for centralized review and analysis is a Security Information Management product.
4. The organization shall integrate analysis of audit records with analysis of performance and network monitoring information to further enhance the ability to identify inappropriate or unusual activity.

DHS-2.16.6.4 Rationale

Gaps and inconsistencies in defenses, unauthorized, and unusual activity may go undetected without appropriate diligence for Audit Monitoring, Analysis, and Reporting within the Resource Custodian and Third Party organizations.

DHS-2.16.7 Audit Reduction and Report Generation

DHS-2.16.7.1 Requirement

The system must provide an audit reduction and report generation capability.

DHS-2.16.7.2 Supplemental Guidance

An audit reduction, review, and reporting capability provides support for near real-time audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents. Audit reduction and reporting tools do not alter original audit records.

DHS-2.16.7.3 Requirement Enhancements

The data management system shall provide the capability to automatically process audit records for events of interest based on selectable event criteria

DHS-2.16.7.4 Rationale

Fast and accurate Audit Reduction and Reporting procedures are critical for mitigating unauthorized and unusual activity in progress.

DHS-2.16.11 Conduct and Frequency of Audits

DHS-2.16.11.1 Requirement

The organization must conduct audits at planned intervals to determine whether the security objectives, measures, processes, and procedures:

1. Conform to the requirements and relevant legislation or regulations
2. Conform to the identified information security requirements
3. Are effectively implemented and maintained
4. Perform as expected
5. Identify inappropriate activities.

DHS-2.16.11.2 Supplemental Guidance

Audits shall be either in the form of internal self-assessment or independent, third party audits. Internal audits, sometimes called first-party audits, are conducted by, or on behalf of, the organization itself for internal purposes. An internal audit must be conducted to ensure that documentation is current with any changes to the system. Independent audits review and examine records and activities to assess the adequacy of security measures, ensure compliance with established policies and operational procedures, and recommend necessary changes in security requirements, policies, or procedures. For independent audits, the auditors need to be accompanied by an appropriate knowledgeable staff person to answer any questions about the particular system under review.

DHS-2.16.11.3 Requirement Enhancements

When auditing a third party for compliance with terms of use for data provided to it, the auditors must be assisted by staff from the organization and third party who are familiar with the policies and procedures governing the data under audit.

DHS-2.16.11.4 Rationale

Gaps and inconsistencies in defenses, unauthorized, and unusual activity may go undetected without appropriate Conduct and Frequency of Audits within the Resource Custodian and Third Party organizations. Periodic reviews will ensure that overall security program evolves to meet any system, technology, or business requirement changes.

DHS-2.16.12 Auditor Qualification

DHS-2.16.12.1 Requirement

The organization's audit program must specify auditor qualifications in accordance with the organization's documented training program.

DHS-2.16.12.2 Supplemental Guidance

The selection of auditors and conduct of audits ensure the objectivity and impartiality of the audit process. Security auditors must:

1. Understand the data management system to be audited and be personally familiar with the system and operating practices
2. Understand the policies and procedures governing the data managed by the system.

DHS-2.16.12.3 Requirement Enhancements

The organization shall assign auditor and system administration functions to separate personnel.

DHS-2.16.12.4 Rationale

Appropriate Auditor Qualifications are required to assess the vulnerabilities and potential impacts of the system. Knowledge of specific technology is required to adequately address issues in-depth (e.g., knowledge of OpenADE).

Appendix A Glossary

Personally Identifiable Information (PII)	Data owned by the Resource Owner that must not be disclosed by a Resource Custodian to any Third Party. A customer's home address and payment information are common examples of PII.
Resource	Data owned by a Resource Owner that may be shared as part of a third-party data access relationship (e.g., the electricity usage data associated with a particular service point).
Resource Custodian	An entity with access to a Resource Owner's resource data that is able to share that data with authorized Third Parties as part of a third-party data access relationship. An electric utility is a common example of a Resource Custodian.
Resource Owner	The rightful owner of a specific piece of resource data (e.g., electric usage data). An electric utility customer is a common example of a Resource Owner.
Shared Resource Key	A token that uniquely identifies an instance of a third-party data access relationship. A Shared Resource Key does not contain any PII.

Subscription	An implementation mechanism representing an agreed-upon schedule or specification of event criteria under which a Resource Custodian provides a Third Party with information regarding a third-party data access relationship.
Third Party	An entity providing some service to a Resource Owner that depends on the availability of the Resource Owner's resource data. A Third Party enters into a data access relationship with the Resource Owner and a Resource Custodian to gain access to the required data.
Third-party Data Access Pattern	A depiction of the interactions among the roles involved in a third-party data access relationship. The pattern describes the behavior of abstract entities (roles), each of which may be implemented by different real entities (actors) in different settings. For example, in one realization of the pattern the Third Party role may be implemented by a value-added service provider, while the same role may be implemented by a retail electric provider in another realization of the pattern. In both cases, the requirements applicable to the Third Party role would apply to the actor filling that role.
Third-party Data Access Relationship	A relationship between a Resource Owner, Resource Custodian, and Third Party in which the Resource Owner authorizes the Resource Custodian to share a specific resource owned by the Resource Owner with the Third Party. Each instance of a third-party data access relationship is identified by a unique Shared Resource Key.

Appendix B Acronyms

3PDA	Third Party Data Access
CFR	Code of Federal Regulations
DHS	Department of Homeland Security
HAN	Home area network
PII	Personally Identifiable Information
REP	Retail Electric Provider
TDSP	Transmission & Distribution Service Provider
UML	Unified Modeling Language
VASP	Value-added Service Provider

Appendix C References

ASAP-SG. (2009, December 14). Security Profile Blueprint. Knoxville, Tennessee, United States of America. Retrieved 1 28, 2010, from Open Smart Grid - OpenSG > SG Security: http://osgug.ucaiug.org/utilisec

National Institute of Standards and Technology. (2009, January). Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (Draft). *NIST Special Publication 800-122 (Draft)* . Gaithersburg, Maryland, United States of America.

OpenADE. (2009, October 23). OpenADE Business and User Requirements v099. Boulder, Colorodo, United States of America.

U.S. Department of Homeland Security. (2009, September). Catalog of Control Systems Security: Recommendations for Standards Developers. Arlington, Virginia, United States of America.

United States Government Accountability Office. (2008, January). Information Security - Protecting Personally Identifiable Information. Washington, District of Columbia, United States of America.