Big Sandy Rural Electric
Cooperative Corporation

504 11th Street
Paintsville, Kentucky 41240-1422
(606) 789-4095 • Fax (606) 789-5454
Toll Free (888) 789-RECC (7322)

RECEIVED
MAR 20 2013

March 19, 2013

MAR 20 2013
PUBLIC SERVICE
COMMISSION

Mr. Jack Conway, Attorney General

1024 Capital Center Drive, Suite 200

Frankfort, KY 40601-8204

RE: Case No. 2012-00428/Consideration of the Implementation of Smart Grid and Smart Meter Technologies

Dear Mr. Conway,

Please find attached the original and fourteen (14) copies of the responses to the Attorney General's Initial Request for information to the Companies in the above referenced case.

If you have any questions, please feel free to contact our office.

Sincerely,

David Estepp, President & General Manager

Big Sandy RECC

DE/jm

Big Sandy Rural Electric
Cooperative Corporation

504 11th Street
Paintsville, Kentucky 41240-1422
(606) 789-4095 • Fax (606) 789-5454
Toll Free (888) 789-RECC (7322)

COMMONWEALTH OF KENTUCKY

BEFORE THE PUBLIC SERVICE COMMISSION

In re the Matter of:

CONSIDERATION OF THE IMPLEMENTATION	)	
OF SMART GRID AND SMART METER	)	**CASE NO.**
TECHNOLOGIES	)	**2012-00428**

RESPONSES TO ATTORNEY GENERAL'S
INITIAL DATA REQUESTS TO THE COMPANIES
DATED FEBRUARY 27, 2013

A Touchstone Energy® Cooperative

Big Sandy Rural Electric
Cooperative Corporation

504 11th Street
Paintsville, Kentucky 41240-1422
(606) 789-4095 • Fax (606) 789-5454
Toll Free (888) 789-RECC (7322)

The undersigned, Jeff Prater, as V.P. Operations and Adam Fg, as IT Manager of Big Sandy Rural Electric Cooperative Corporation being first duly sworn, states that the responses to the Attorney General's Initial Data Requests in Case No. 2012-00428 dated February 27, 2013, herein are true to the best of my knowledge and belief formed after reasonable inquiry.

Dated: March 18, 2013

Subscribed, sworn to, and acknowledged before me by Jeff Prater and Adam Ferguson on behalf of said Corporation this 18th **day of** March **in the year of 2013.**

Notary Public: Judy L. McClure
My Commission Expires: 06-19-14

Request 1
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 1: Since the Commission initiated Consideration of *the New Federal Standards of the Energy Independence and Security Act of 2007*, Administrative Case No. 2008-00408, has the company changed its position regarding Smart Grid? If so, how?

RESPONSE 1: Big Sandy RECC references the response to AG Request 1 submitted by EKPC and adopts that response as its own.

Request 2
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 2: Are the technologies pertaining to the implementation of Smart Grid definitely known and proven?

a. If yes, explain in detail every aspect from the use of each technology from the company to the end-user.

b. If not, explain in detail what technologies are already advancing/improving as well as those that are envisioned on the immediate time horizon.

RESPONSE 2: Yes, in our situation the technologies implemented by Big Sandy are known and proven. Big Sandy RECC has a fully implemented AMI metering system. Big Sandy RECC's does have very limited exposure, but our power line carrier has been a benefit to both the coop and our consumers. The system has done away with the outdated techniques of our consumers reading their own meters.

Request 3
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 3: In light of resent catastrophic storms over the past ten years (for example, the various ice storms, tornadoes, and strong winds), which electric companies have experienced, and for which the company may ultimately have sought regulatory assets, can the company affirmatively state that its basic infrastructure, including all of its generation, transmission and distribution facilities, have proven to be reliable 24 hours a day, seven days a week, 365 days a week? If not, for each and every storm that it affected the utility in excess of two days, please provide the following:

a. The number of days before the company's last ratepayer's electricity was restored for each storm.

b. The average number of days, or hours if applicable, that the average ratepayer's outage lasted for each storm.

c. The average financial loss for the average ratepayer for each storm, if known.

RESPONSE 3: Although our reliability is near 100%, it is beyond the design of any infrastructure to withstand a major storm. Therefore, it would be impossible for Big Sandy RECC to affirmatively state that its basic infrastructure, including all of its distribution facilities, have proven to be reliable 24 hours a day, seven days a week, 365 days a year.

Big Sandy RECC just implemented an Outage Management System (OMS) in January 2012. Consequently, it is not practical to retrieve such data prior to this date. However, the information from the 2012 tornado was captured on the OMS system and we are providing this data.

a. It took 12 days for Big Sandy RECC to restore power to our last rate paying consumer after the 2012 tornado.
b. The average number of hours that the average rate payer experienced was 7 hours during the 2012 tornado.
c. This amount is unknown, as our OMS does not track financial statistics.

Request 4
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 4: Does the company agree with the Attorney General that electricity is not considered a luxury service but a necessary commodity of modern life? If not, why not?

RESPONSE 4: Big Sandy RECC references the response to AG Request 4 submitted by EKPC and adopts that response as its own.

Request 5
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 5: Does the company agree that the fundamental reliability of its electric grid- i.e., the delivery of electricity to the end-user 24/7/365- is paramount to the end-user's ability to monitor and/or conserve his/her demand or electricity consumption? If not, why not?

RESPONSE 5: Big Sandy RECC references the response to AG Request 5 submitted by EKPC and adopts that response as its own.

Request 6
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 6: Please state whether the company is aware of any cyber security breaches affecting the electric and gas industries that have either occurred in the United States or internationally. If the answer is in the affirmative, please explain the details of the breaches without exposing information that is not already in the public domain.

RESPONSE 6: Big Sandy is **not** aware of any cyber security breaches affecting the electric and gas industries that have either occurred in the United States or internationally.

Request 7
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 7.: Please confirm that the company is aware that the prior United States Secretary of Defense Leon Panetta, in speaking on the vulnerability of the nation's electric grid with the consequential safety and security concerns that ensue, warned the Senate Appropriations Committee on Defense that the risk to the United States could even be considered the equivalent of a "digital Pearl Harbor".

a. Is this concern of the vulnerability of the nation's electric grid shared by the company? If not, why not?

RESPONSE 7: Yes, Big Sandy RECC does share the concern of the vulnerability of the nation's electric grid. Concerns about cybersecurity have actually grown with the deployment of smart grid technologies, which typically means using digital communication devices with common technical standards and getting rid of some analog systems so that data can flow in large volumes and quickly. This could lead to a hodgepodge of legacy and modern equipment in the transmission and distribution networks that don't work well together. That also makes it difficult to implement rules and security technologies that have to perform effectively across the networks.

Request 8
Page 1 of 1
Witness: Big Sandy: ADAM FERGUSON

Request 8: With regard to cybersecurity in general, can the company unequivocally confirm that its system reliability is not vulnerable to a cybersecurity attack? If not, what could be the consequences? Please explain in detail as much as possible for the following:

a. the company, and
b. the company's rate pay

RESPONSE 8: No, Big Sandy RECC isn't 100% reliable against cyber-attacks. What can be lost is names and address up to SSN # and banking accounts numbers of both employees and ratepayers.

Request 9
Page 1 of 1
Witness: Big Sandy: ADAM FERGUSON

Request 9: Please provide the names of the standards, protocols or policies which the company observes and/or implements in its maintaining its system reliability from cyber security threats.

RESPONSE 9: Big Sandy has put in place and follows Red flag rules and has put in place (IPS) Intrusion Prevention Service by Dell Secureworks who monitors outside of our firewall (Cisco 5510 series). Along with anti-virus software that's on all computers and servers.

Request 10
Page 1 of 1
Witness: Big Sandy: ADAM FERGUSON

Request 10: Please provide copies of the standards, protocols or policies which the company observes and/or implements in its maintaining its system reliability from cyber security threats.

RESPONSE 10: Big Sandy RECC's response to request #10 is attached as Exhibit A.

Request 11
Page 1 of 1
Witness: Big Sandy: ADAM FERGUSON

Request 11: With regard to cybersecurity in general, can the company unequivocally confirm that its ratepayers' privacy of data cannot be compromised or otherwise divulged to any individual or entity not associated with the company, or a qualified third-party which has issues a non-disclosure statement or the ratepayers? If not, what could be the consequences? Please explain in detail as much as possible for the following:

a. the company, and

b the company's ratepayers.

RESPONSE 11: Big Sandy RECC and third-party (SEDC) can only put in place standards and policies along with passwords to help prevent loss of ratepayer's privacy of data and company data. Consequences can be is names and address up to SSN # and banking accounts numbers of both employees and ratepayers.

Request 12
Page 1 of 1
Witness: Big Sandy: ADAM FERGUSON

Request 12: If a qualified third-party that has agreed to a non-disclosure statement and obtains ratepayers' private information, what guarantees exist that the information will not be disclosed, whether intentionally or unintentionally?

RESPONSE 12: There is no guarantee with third-party (SEDC). There are only Standards protocols and policies put in place by SEDC that only helps prevent loss of data.

Request 13
Page 1 of 1
Witness: Big Sandy: ADAM FERGUSON

Request 13: Please provide the names of the standards, protocols or policies which the company observes and/or implements in its maintaining its ratepayers' privacy data from cyber security threats.

RESPONSE 13: We have put in place and follow Red flag rules and have also put in place (IPS) Intrusion Prevention Service by Dell Secureworks who monitors outside of our firewall (Cisco 5510 series). Along with anti-virus software that's on all computers and servers.

Request 14
Page 1 of 1
Witness: Big Sandy: ADAM FERGUSON

Request 14: Please provide copies of the standards, protocols or policies which the company observes and/or implements in its maintaining its ratepayers' privacy data from cyber security threats.

RESPONSE 14: Big Sandy RECC has provided the documents as requested in #14 as Exhibits B, C, D, E and F attached to this document.

Request 15
Page 1 of 1
Witness: Big Sandy: ADAM FERGUSON

Request 15: Given the vulnerability of the electric grid to cyberattacks, describe what analog (non-digital) means the company will have in place to insure reliability, including but not limited to the maintenance of legacy systems.

RESPONSES 15: Don't really understand the question. With our AMI (Aclara) system we only have in place digital commutations.

Request 16
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

<u>Request 16:</u> What are the company's estimated costs to invest in order to fully implement Smart Grid?

a. Do any cost estimates include results of any modeling that may show the degree of exposure to the following risks: (a) hacking; (b) electronic magnetic pulses (EMPs, whether related to solar flares or otherwise); and/or (c) weather events? If so, provide a list of the modeling software used to produce any estimates, the scenarios and sensitivities examined, and any and all such results.

<u>RESPONSE 16:</u> Big Sandy RECC references the response to AG Request 16 submitted by EKPC and adopts that response as its own.

Request 17
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 17: Please explain in detail what benefits, if any, the company expects its ratepayers to realize because of Smart Grid?

a. Does the company believe that societal benefits are to be considered in evaluating benefits? If so, detail those societal benefits and how they may be used in evaluations? If not, why not?

RESPONSE 17: Big Sandy RECC references the response to AG Request 17 submitted by EKPC and adopts that response as its own.

Request 18
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 18: Would the company agree to strict limits and/or caps on ratepayer costs? If not, why not?

RESPONSE 18: Big Sandy RECC references the response to AG Request 18 submitted by EKPC and adopts that response as its own.

Request 19
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 19: Would the company agree to allow ratepayers to opt-out of smart meter deployment? If not, why not?

RESPONSE 19: Big Sandy RECC references the response to AG Request 19 submitted by EKPC and adopts that response as its own.

Request 20
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 20: Can the company quantify measureable and significant benefits that the ratepayers will realize, including a monetary quantification of net savings (if any) to ratepayers?

RESPONSE 20: Big Sandy RECC references the response to AG Request 20 submitted by EKPC and adopts that response as its own.

Request 21
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 21: Please explain in detail what detriments, if any, the company expects its ratepayers to realize because of Smart Grid? Include in the explanation both new costs as well as stranded costs.

RESPONSE 21: Big Sandy RECC references the response to AG Request 21 submitted by EKPC and adopts that response as its own.

Request 22
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 22: What are the company's estimated costs which the company expects the ratepayers to realize?

RESPONSE 22: Big Sandy RECC references the response to AG Request 22 submitted by EKPC and adopts that response as its own.

Request 23
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 23: What are the company's estimated costs which the company expects its shareholders, if any, to realize? Include in the explanation both new costs as well as stranded costs.

RESPONSE 23: Big Sandy RECC references the response to AG Request 23 submitted by EKPC and adopts that response as its own.

Request 24
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 24: Does the company agree that its costs to invest and implement Smart Grid will be different than other utility companies? If not, why not?

RESPONSE 24: Big Sandy RECC references the response to AG Request 24 submitted by EKPC and adopts that response as its own.

Request 25
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 25: Does the company agree that its ratepayers' benefits, whether financial or otherwise, may differ from one utility to another upon implementation of any Smart Grid technology? If not, why not?

RESPONSE 25: Big Sandy RECC references the response to AG Request 25 submitted by EKPC and adopts that response as its own.

Request 26
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 26: Can the company guarantee that the deployment of Smart Grid will not interfere with the regulatory compact whereby the ratepayers will receive safe, adequate and reliable service at fair, just and reasonable costs? If not, why not? Explain in detail.

RESPONSE 26: Big Sandy RECC references the response to AG Request 26 submitted by EKPC and adopts that response as its own.

Request 27
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 27: Answer the above question with the definition of "fair, just and reasonable costs" as being economically feasible for the end-user. East Kentucky Power.

a. Provide any cost-benefit analysis that the company has run or will run to make the determination of economically feasible to the end-user.

RESPONSE 27: Big Sandy RECC references the response to AG Request 27 submitted by EKPC and adopts that response as its own.

Request 28
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 28: Regarding time of use (TOU) rates, can the company confirm that low-income ratepayers will not be disproportionately affected more than non-low-income customers? If not, why not? (Provide in the answers in any studies, reports, analyses and relevant data.)

RESPONSE 28: Big Sandy has **not** performed any studies or analyses on TOU. If a consumer is low-income due to government assistance, then they would have more flexibility to regulate their time of usage because they would be home 24/7. Consequently, this could pose as a potential benefit to them.

Request 29
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 29: With regard to TOU rates, does the company have any history with any such programs? If so, explain in detail with particular facts as to:

a. the number of customers who participated;

b. whether they remained on the program;

c. whether they saved money on their bills; and

d. whether the customers ultimately reduced their usage.

RESPONSE 29: Big Sandy RECC has no history with regard to TOU rates.

Request 30
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 30: What proposals will the company present to deal with technological impediments to the broad use of Smart Grid, including but not limited to the following:

a. low and fixed-income individuals who do not have Internet resources at their home;

b. multiple forms of telecommunications technology used to access information (i.e., analog, cellular, VOIP); and

c. multiple and proprietary technology and software options in the market that may lead to issues of compatibility?

RESPONSE 30: Big Sandy RECC has applied for pre pay metering system and is currently waiting upon approval from the Kentucky Public Service Commission. Many of these concerns were addressed during this process. It was Big Sandy RECC's stand that internet service was not mandatory to participate in pre pay metering. Our modes of communication were set as: email, text, or automated phone messages.

Plus, Big Sandy RECC has a fully implemented AMI metering system. However, our consumers are still provided with a hard copy of their billing each month. Thus, this implementation does not change our communication forms with our consumers – it remains the same as pre implementation.

These two situations are the only ones that Big Sandy RECC has faced concerning the above mentioned issues. Furthermore, we do not for see any technological impediment in providing electric service with current AMI System.

Request 31
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 31: Assume: Full deployment of Smart Grid at the residential ratepayer level consisting of a household with only Energy Star appliances, an HVAC system with at least a 15 SEERS rating, etc. and any smart grid apparatuses/equipment for interconnectivity with the electricity provider (including generation, transmission and distribution). East Kentucky Power

a. Does the company agree that if full deployment of the magnitude described in the above question occurs, the average residential ratepayer could experience a significant capital outlay?

b. If so, what are the projected costs?

c. If no costs are anticipated by the electric provider, why not?

RESPONSE 31: Big Sandy RECC references the response to AG Request 31 submitted by EKPC and adopts that response as its own.

Request 32: In regard to appliances, such as refrigerators or lighting, does the company agree that in the long run, it is cheaper for the end-user himself/herself to make that capital outlay for the purchase of the appliance or lighting than have the company provide the appliance(s) and build the costs into the company's ratebase which would then include a profit component for the company on an on-going basis?

RESPONSE 32: Big Sandy RECC references the response to AG Request 32 submitted by EKPC and adopts that response as its own.

Request 33
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 33: Confirm that the Smart Grid depends, at least in part, if not exclusively, on telephony (whether landline, fiber optic, wireless or VOIP) at the end-user level for the end-user to participate in his/her altering his/her electricity usage patterns or behavior.

RESPONSE 33: Please refer to Big Sandy RECC's **RESPONSE 30** above.

Request 34
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 34: If the answer to the above question is in the affirmative, confirm that limited access or even complete absence of access to telephony will interfere with, if not prevent, the deployment of the Smart Grid at the end-user level.

RESPONSE 34: Big Sandy RECC's would not be unable to answer this question at this time. As, we have no first-hand experience regarding this matter that pertains to the end-user level.

Request 35
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 35: If the company intends to install infrastructure/software allowing for the transmission of Smart Grid/Smart Meter data over its distribution/transmission conductors and networks, provide estimates, or actual numbers, for the costs of doing so.

RESPONSE 35: Big Sandy RECC fully implemented an AMI system in 2008. As this implementation took place close to 5 years ago, the retrieval of actual numbers is not feasible. Therefore, Big Sandy RECC's estimated costs for this project were $246.00 per metering point.

Request 36
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 36: Is there a standard communications' protocol that the company will deploy in its Smart Grid that will be interoperable regardless of the communications provider?

a. If not, explain how the company plans on addressing any problems that might arise.

RESPONSE 36: Our communications' protocol is established by Aclara. They offer a unique protocol that links the meter to the substation receiver. Any modern communications may be used including, but not limited to, broadband, internet, DSL, satellite DSL, traditional phone lines, etc. to connect with the substation receiver.

Request 37
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

<u>Request 37:</u> If improved reliability is the goal of Smart Grid/Smart Meter, would it not be more cost-effective to invest in infrastructure hardening (for example, utilizing protocols and standards developed and implemented by many utilities in hurricane-prone regions)?

<u>RESPONSE 37:</u> Big Sandy RECC references the response to AG Request 37 submitted by EKPC and adopts that response as its own.

Request 38
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 38: Describe the company's plans to avoid obsolescence of Smart Grid/Smart Meter infrastructure (both hardware and software) and any resulting in stranded costs. (This question and the subparts should be construed to relate to both the Smart Grid Investment Standard as well as the Smart Grid Information Standard.) East Kentucky Power

a. Describe who would pay for stranded costs resulting from obsolescence.

b. With regard to the recovery of any obsolete investment, explain the financial accounting that should be used (as in account entry, consideration of depreciation, time period involved, etc.).

RESPONSE 38: Big Sandy RECC references the response to AG Request 38 submitted by EKPC and adopts that response as its own.

Request 39
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 39: With regard to interoperability standards, does the company agree that Smart Grid equipment and technologies as they currently exist, and are certain to evolve in the future, are not a one size fits all approach to the Commonwealth?

RESPONSE 39: Big Sandy RECC references the response to AG Request 39 submitted by EKPC and adopts that response as its own.

Request 40
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 40: Is dynamic pricing strictly defined as TOU? East Kentucky Power

a. If not, explain why not.

b. Is the company requesting that dynamic pricing be voluntary or involuntary, if at all?

RESPONSE 40: Big Sandy RECC references the response to AG Request 40 submitted by EKPC and adopts that response as its own.

Request 41
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 41: Please explain in detail whether the company has any dynamic programs in place in Kentucky.

a. For each program, provide the number of participants.

b. For each program, state whether those participants on aggregate have saved costs on their bills.

c. For each program, state whether those participants on aggregate have saved costs on their bills.

d. For each program, state whether each participant has saved costs on his/her/its bills. (The question is not intended to request any private identifier information.)

RESPONSE 41: Big Sandy RECC has no dynamic pricing programs.

Request 42
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 42: Does the company recommend the Commission to formally adopt the EISA 2007 Smart Grid Investment Standard? If not, why not?

RESPONSE 42: Big Sandy RECC references the response to AG Request 42 submitted by EKPC and adopts that response as its own.

Request 43
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 43: Does the company recommend the Commission to formally adopt the EISA 2007 Smart Grid Information Standard? If not, why not?

RESPONSE 43: Big Sandy RECC references the response to AG Request 43 submitted by EKPC and adopts that response as its own.

Request 44
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 44: Does the company recommend issuing an IRP Standard?

a. If so, what concerns does the company have with a standard, including "priority resource," especially as it relates to cost-effectiveness? East Kentucky Power

b. What concerns would the company have with a standard as it affects CPCN and rate applications?

RESPONSE 44: Big Sandy RECC references the response to AG Request 44 submitted by EKPC and adopts that response as its own.

Request 45
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 45: Does the company agree that any investment in grid modernization infrastructure should be done before deploying TOU rates or dynamic pricing? If not, why not?

RESPONSE 45: Big Sandy RECC references the response to AG Request 45 submitted by EKPC and adopts that response as its own.

Request 46
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 46: Regarding the Kentucky Smart Grid Roadmap Initiative (KSGRI), does the company believe that it provides the fundamental basis for the Commonwealth as a whole to proceed with Smart Grid given its lack of incorporating all electric utilities such as municipalities and the TVA, along with its distribution companies? If yes, please explain why. If not, please explain why not.

RESPONSE 46: Big Sandy RECC references the response to AG Request 46 submitted by EKPC and adopts that response as its own.

Request 47
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 47: Does the company believe that the Commonwealth's electric industry is, or will become, so interconnected that all electric entities in any way involved or associated with the generation, transmission and/or distribution of electricity should be included and participate to some degree with Smart Grid if it is to come to fruition? If yes, please explain why. If not, please explain why not.

RESPONSE 47: Big Sandy RECC references the response to AG Request 47 submitted by EKPC and adopts that response as its own.

Request 48
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 48: Does the company believe that any Smart Grid Investment will trigger a CPCN case? If not, why not?

RESPONSE 48: Big Sandy RECC references the response to AG Request 48 submitted by EKPC and adopts that response as its own.

Request 49
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 49: Does the company believe that Dynamic Pricing should be economically feasible for the end-user and be supported by a cost- benefit analysis?

RESPONSE 49: Big Sandy RECC references the response to AG Request 49 submitted by EKPC and adopts that response as its own.

Request 50
Page 1 of 1
Witness: Big Sandy: JEFF PRATER

Request 50: If additional education is contemplated with the deployment of the Smart Grid, please explain in detail if known or contemplated.

RESPONSE 50: Big Sandy RECC references the response to AG Request 50 submitted by EKPC and adopts that response as its own.

SEDC
Southeastern Data Cooperative

TO: ALL SEDC MEMBERS
FROM: RON CAMP
SUBJECT: INDENTITY THEFT AND RED FLAG RULES
DATE: OCTOBER 10, 2008

In the last month, we have received numerous inquiries on SEDC's position on the Red Flag Regulations. As of late, emails have been circulating as to how best to address these issues as a group. Due to this activity, I am writing to explain our position on the Red Flag Regulations (referred to as rules) and how we can be of assistance to our members.

As far as we can tell, SEDC is not really a part of the Red Flag guidelines. These regulations need to be addressed by each utility except for the requirement for "Oversight" of a third party service provider. For this reason, I am attaching an SEDC Red Flag Service Provider Oversight document along with relevant policy documents. These documents will be enforced with regard to SEDC employee access to the data of your members, whether access is through dial-in, request for databases, or information submitted by your employees in the form of printed material. It is SEDC's intent for this documentation to satisfy your utility's oversight requirement.

From a practical point of view, however, we realize we must be part of any change you feel needs to be made in the software that reflect your individual utility's need to comply with the FTC ruling. Here in lies the problem faced by all software development companies regarding the FTC regulations. We are not aware of any specific software specifications of a regulatory nature that dictate required software changes of any kind. These regulations, in comparison to the PCI requirements which, to the credit of the credit card companies, are very clear, the FTC's Red Flag Rules are not clear or specific.

Of course, we at SEDC want to be as helpful in making changes as we can, but as of this writing, we have over 200 separate groups deciding the interpretation of these rules and how to comply. In fact, a central theme of the Red Flag Rules is that each creditor-utility organization is to design and implement a program appropriate to their size and complexity as well as the nature of their operations. In short, there is no one size fits all.

For this reason, I ask that all requests for software changes on this matter be submitted to our advisory committee for consideration. There needs to be a clearing house for these issues. In no way does SEDC want to appear to be the limiting factor in utilities achieving what they feel must be done; however, it needs to be understood that left unorganized the number and nature of these requests could create an unmanageable workload for SEDC that would not be necessary or in the best interest of all members.

SEDC has already begun some logical changes, such as masking SSN numbers on screens, and we will continue to evaluate requested changes as to need and scope of effort. The utility would always have the option to have specific changes not recommended by the advisory committee done by contractors and incorporated into the code if they are of the mind that the issue is critical to their program.

I hope this letter outlines what we all feel is necessary to address such an undefined task. Please be assured we will continue to work with our members in every way possible.

Sincerely,

Ron Camp

DELL SecureWorks

Service Organization Controls 1 Report

Dell SecureWorks' Description of Controls for Counter Threat Platform Managed Security Services

For the period May 1, 2012 through October 31, 2012
with Independent Service Auditor's Report Including Tests
Performed and Results Thereof

Table of Contents

Independent Service Auditor's Assurance Report

PRIVATE AND CONFIDENTIAL

This report is intended solely for the management of Dell SecureWorks, the customers of Dell SecureWorks and the independent auditors of Dell SecureWorks. .

ERNST & YOUNG

Ernst & Young LLP
Suite 1000
55 Ivan Allen Jr. Boulevard
Atlanta, GA 30308

Tel: +1 404 874 8300
Fax: +1 404 817 5589
www.ey.com

Section I – Independent Service Auditor's Assurance Report

Board of Directors
Dell SecureWorks

Scope

We have examined Dell SecureWorks' accompanying Description of Dell SecureWorks' Controls for the Counter Treat Platform (CTP) supporting Dell SecureWorks Managed Security Services (MSS) system throughout the period May 1, 2012 to October 31, 2012 (Description) and the suitability of the design and operating effectiveness of controls described therein to achieve the related control objectives stated in the Description. The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls contemplated in the design of Dell SecureWorks' controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Dell SecureWorks uses certain subservice organizations to provide certain services listed in Appendix A. The Description includes only the controls and related control objectives of Dell SecureWorks and excludes the control objectives, and related controls of the subservice organizations listed in Appendix A. Our examination did not extend to controls of the organizations listed in Appendix A.

The information in the accompanying Other Information Provided by Dell SecureWorks is presented by management of Dell SecureWorks to provide additional information and is not part of Dell SecureWorks' Description. Such information has not been subjected to the procedures applied in our examination and, accordingly we express no opinion on it.

Dell SecureWorks' responsibilities

Dell SecureWorks has provided the accompanying assertion titled, Report of Management on Dell SecureWorks, Inc. Counter Threat Platform Managed Security Services (Assertion) about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls described therein to achieve the related control objectives stated in the Description. Dell SecureWorks is responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion, providing the services covered by the Description, specifying the control objectives and stating them in the Description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the Assertion, and designing, implementing, and documenting controls to achieve the related control objectives stated in the Description.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the related control objectives stated in the Description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the Description is fairly presented and the controls described therein are suitably designed and operating effectively to achieve the related control objectives stated in the Description throughout the period May 1, 2012 to October 31, 2012.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls described therein to achieve the related control objectives stated in the Description involves performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives. Our procedures included assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives were achieved. An examination engagement of this type also includes evaluating the overall presentation of the Description, the suitability of the control objectives, and the suitability of the criteria specified by the service organization and described in the Assertion. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of user entities and their independent auditors and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in Managed Security Services provided by Dell SecureWorks. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become ineffective or fail.

Opinion

In our opinion, in all material respects, based on the criteria described in Dell SecureWorks' Assertion:

a. the Description fairly presents the CTP MSS system that was designed and implemented throughout the period May 1, 2012 to October 31, 2012.

b. the controls related to the control objectives stated in the Description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period May 1, 2012 to October 31, 2012 and if user entities applied the complementary user entity controls contemplated in the design of Dell SecureWorks' controls and if subservice organizations applied the controls contemplated in the design of Dell SecureWorks' controls throughout the period May 1, 2012 to October 31, 2012.

c. the controls tested, which together with the complementary user entity controls and subservice organizations' controls referred to in the scope paragraph of this report if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period May 1, 2012 to October 31, 2012.

Description of tests *of* controls

The specific controls tested and the nature, timing, and results of those tests are listed in the accompanying Description of Control Objectives, Controls, Tests and Results of Tests section (Description of Tests and Results).

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Dell SecureWorks, user entities of Dell SecureWorks' CTP MSS system during some or all of the period May 1, 2012 to October 31, 2012, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Ernst + Young LLP

November 12, 2012
Atlanta, GA

Dell SecureWorks' Assertion

DELL SecureWorks

Section II – Dell SecureWorks' Assertion

November 12, 2012

We have prepared the accompanying Description of Dell SecureWorks' Controls for the Counter Threat Platform (CTP) supporting Dell SecureWorks Managed Security Services (Description) of Dell SecureWorks (Service Organization) for users of the system during some or all of the period May 1, 2012 to October 31, 2012 (user entities)_and their independent auditors who have a sufficient understanding to consider the Description, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. The management of Dell SecureWorks confirms, to the best of its knowledge and belief, that:

a. the Description fairly presents the CTP Managed Security Services system (System) made available to user entities during the period May 1, 2012 to October 31, 2012. Managed Security Services provided by Dell SecureWorks uses various subservice organizations to provide backup tapes storage services and various inspection and maintenance services. The Description includes only the controls and related control objectives of the Service Organization and excludes the control objectives, and related controls of subservice organizations listed in Appendix A. The criteria we used in making this assertion were that the Description:

   (1) presents how the System made available to user entities was designed and implemented, including:

   - the types of services provided;
   - the procedures, within both automated and manual systems, by which those services are provided to user entities;
   - how the System captures and addresses significant events and conditions;
   - the process used to prepare reports or other information provided to user entities;
   - specified control objectives and controls designed to achieve those objectives;
   - controls that, in designing the System, we contemplated would be implemented by user entities in order to achieve the specified control objectives (Complementary User Entity Controls);
   - other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to the services provided.

   (2) does not omit or distort information relevant to the scope of the System, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities and their independent auditors, and may not, therefore, include every aspect of the System that each individual user entity and its

independent auditor may consider important in the user entity's own particular environment.

b. the Description includes relevant details of changes to the System during the period from May 1, 2012 to October 31, 2012.

c. the controls related to the control objectives stated in the Description, which together with the complementary user entity controls and subservice organizations' controls referred to above if suitably designed and operating effectively, were suitably designed and operated effectively throughout the period May 1, 2012 to October 31, 2012 to achieve those control objectives. The criteria we used in making this assertion were that

(1) the risks that threaten the achievement of the control objectives stated in the Description have been identified by the service organization;

(2) the controls identified in the Description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved; and

(3) the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Dell SecureWorks

Dell's Description of Service Organization Controls for Counter Threat Platform Managed Security Services

For the period May 1, 2012 through October 31, 2012

Section III – Dell's Description of Service Organization Controls for Counter Threat Platform MSS

For the period May 1, 2012 through October 31, 2012

Overview of Operations

Dell SecureWorks is a provider of information security services with more than 3,200 customers worldwide. Organizations of all sizes, including more than 15 percent of the Fortune 500, rely on Dell SecureWorks to protect their assets, support compliance and reduce costs. The combination of security knowledge and expertise, purpose-built security technology and processes, and excellent customer service makes Dell SecureWorks one of the premier providers of information security services. Positioned in the Leader's Quadrant of Gartner's Magic Quadrant for Managed Security Service Providers (MSSP) and recognized as a Leader in the latest Forrester Wave, Dell SecureWorks has been recognized by SC Magazine's readers with the "Best Managed Security Service" award for 2006, 2007, 2008, 2009 and 2011, and has been named to the Inc. 500, Inc. 5000 and Deloitte lists of fastest-growing companies.

Dell SecureWorks was founded in 1999 to protect organizations from Internet threats. A pioneer in the industry, Dell SecureWorks has grown by combining advanced technology with security expertise to offer organizations a broad array of award-winning information security services.

In February of 2011, SecureWorks was acquired by Dell, Incorporated (Inc.) to expand its portfolio of enterprise-class Information Technology (IT)-as-a-Service solutions. As part of the acquisition certain business functions, such as certain legal, accounting and Human Resources (HR) functions, have been integrated into Dell corporate functions.

Description of services provided by Dell SecureWorks

Managed Network IDS/IPS

Dell SecureWorks' Managed Intrusion Prevention and Detection service (IDS/IPS) provides full lifecycle management of network IPS and IDS devices to ensure optimum performance and protection. Using intelligence from the Dell SecureWorks' Counter Threat Unit, certified experts fine-tune countermeasures to their customers' environment in order to protect against the latest threats. IPS and IDS alerts are monitored, correlated and assessed in real time by Dell SecureWorks' Security Analysts, who identify threats and respond accordingly to protect the customers' critical assets. Dell SecureWorks' Managed IDS/IPS service supports existing deployment of IDS/IPS infrastructure, as well as several other market-leading products. Dell SecureWorks' proprietary iSensor IPS solution can also be included in the service as a cost-effective, fully managed bundle.

Features of this service include:

- 24x7x365 real-time monitoring by Global Information Assurance Certification (GIAC) certified security experts
- Real-time blocking of malicious Internet activity before compromise
- Proactive administration, signature tuning and maintenance
- Countermeasure deployment based on industry-leading threat visibility
- On-demand security, board-level and compliance reports

Managed IDS/IPS with iSensor

For organizations seeking to implement IDS/IPS technology or upgrade their infrastructure, Dell SecureWorks offers a cost-effective product and service bundle using iSensor IPS appliances. Dell SecureWorks provides full lifecycle management of iSensor devices, from design and implementation to ongoing management and monitoring. Managed IDS/IPS with iSensor features include:

- Site review, planning and IDS/IPS implementation
- Real-time prevention of threats
- 24x7x365 real-time analysis of events by GIAC GCIA (Global Certified Intrusion Analyst) certified security analysts
- High-fidelity signatures developed by the Counter Threat Unit (CTU) based on industry-leading threat visibility
- Advanced correlation across all log and event sources, vulnerability scanning data and threat intelligence
- Statistical analysis and anomaly detection
- On-demand security, board-level and compliance reports
- Unlimited and unmetered expert support and recommendations

Managed Firewall

Dell SecureWorks' Firewall Management service provides 24x7x365 proactive administration, monitoring and maintenance of firewall infrastructure. The Firewall Management service is tailored to each customer's environment, leveraging proven practices to ensure appropriate network access while preserving the availability, integrity and privacy of information. Dell SecureWorks' certified analysts monitor firewall health events and traffic logs in real time, identifying threats before they impact critical assets and alerting response personnel. Dell SecureWorks supports both, the traditional Managed Services model, where customers have limited or no administrative privileges for the Managed Firewall, as well as a co-managed services model, where customers retain ownership and administrative rights to their firewalls to the extent that they prefer. This service includes:

- Firewall installation, configuration, auditing and maintenance
- Total lifecycle management including performance and troubleshooting
- 24x7 firewall monitoring to detect known and unknown threats
- Concise easy to understand reporting

Managed Web Application Firewall

To help organizations protect their web applications, Dell SecureWorks' Managed Web Application Firewall service provides 24x7x365 management and real-time monitoring for Web Application Firewalls. Leveraging years of security experience, analysts can support the entire Web Application Firewall (WAF) lifecycle including:

- Solution design and deployment
- Continuous tuning and configuration management
- Real-time event monitoring and analysis
- Maintenance, backup and recovery
- Performance and availability management
- Comprehensive security and compliance reporting

Managed Host Intrusion Prevention

Dell SecureWorks' Managed Host Intrusion Prevention Service protects systems from attacks that can damage applications, data, or the underlying operating system. This service delivers protection at the host level by blocking behavior that signals malicious activity. This service includes:

- Real-time behavior-based attack blocking
- Protection against attacks that bypass perimeter security
- Policy set management, automatic updates and all other maintenance
- 24x7x365 real-time monitoring and response
- Comprehensive reporting

Log Monitoring

Dell SecureWorks' Log Monitoring Service provides 24x7x365 vigilance over critical information assets. Dell SecureWorks' security analysts monitor, analyze and respond to security events from security devices, network infrastructure, servers, databases, applications or any other critical information asset in real-time. Service features include:

- Expert analysis by GIAC GCIA certified team of Security Analysts
- Vendor neutral, infrastructure-wide coverage
- Real-time, 24x7 monitoring, correlation and incident response
- Risk discovery with remediation details and workflow with ticketing
- On-demand security and compliance reports through the real-time customer Portal
- Unlimited support from security experts for many managed services

Managed Log Retention

Dell SecureWorks' Managed Log Retention helps organizations satisfy security and compliance requirements for log collection, storage and reporting without the management overhead and capital expense required for log management products. Leveraging Dell SecureWorks' LogVault, LogLogic and Arcsight technology, Managed Log Retention is a cost-effective option that integrates seamlessly with other Managed Security Services to provide customers with comprehensive security and compliance solutions. This service:

- Satisfies log retention requirements for North American Energy Reliability Corporation (NERC CIP), Payment Card Industry (PCI) security standards, Federal Financial Institutions Examination Council (FFIEC), Sarbanes-Oxley (SOX) and other regulations

- Provides on-demand access to all raw log data
- Supports security and network troubleshooting
- Maintains forensically sound log data for investigation and court proceedings
- Features no management or maintenance overhead
- Integrates seamlessly with other services for total security and compliance solutions

Security Information Management (SIM) On-Demand

Dell SecureWorks' SIM On-Demand Service allows organizations to attain all the benefits of SIM technology, without experiencing the drawbacks of installing, managing and maintaining a complex SIM deployment. Dell SecureWorks' SIM On-Demand Service delivers event aggregation, correlation and reporting "in-the-cloud," requiring no lengthy software implementations. The SIM On-Demand service can be up and running in a matter of days, immediately presenting actionable information, a consolidated view of the security status of critical assets and on-demand compliance reports via the secure web-based Dell SecureWorks Portal. Service features include:

- Rapid implementation and no management overhead
- Vendor neutral, infrastructure-wide event aggregation and advanced correlation
- Asset classification, remediation workflow and 24x7 access to Dell SecureWorks' security experts
- On-demand security and compliance reports through Dell SecureWorks' real-time customer Portal

Vulnerability Management

Dell SecureWorks' Vulnerability Management service identifies exposures and weak spots in customer environments by performing external scanning and internal scanning across the network. Provided as an on-demand service, Vulnerability Management enables vulnerability scanning without the hardware, software and maintenance requirements of scanning products. Vulnerability results can be integrated into Dell SecureWorks' other Managed Security Services, allowing threats against vulnerable and non-vulnerable systems to be assessed and prioritized accordingly. Features of this service include:

- Deep internal and external scanning
- Highly accurate results using vulnerability "chaining" and exploit confirmation
- Detailed remediation guidance
- On-demand security and compliance reports

Web Application Scanning

Leveraging Qualys web application scanning technology, the Web Application Scanning service proactively audits the security of web applications and their backend databases to identify flaws that could be exploited by attackers. Provided on-demand, Web Application Scanning helps organizations safeguard web applications, protect sensitive data and satisfy regulatory requirements. Service features include:

- Comprehensive Web application scanning

- Discovery of SQL Injection flaws, Cross-site scripting, etc.
- Detection of sensitive content in HTML (Card data, SSNs, etc.)
- Support for dynamic Web 2.0 technologies including JavaScript, AJAX and Flash
- Use of browser emulation to find and test all links
- Includes database scanning

Threat Intelligence Service

The Dell SecureWorks Counter Threat Unit (CTU) performs in-depth analysis of emerging threats and Zero-Day vulnerabilities. The CTU specializes in malware analysis, reverse engineering, counter intelligence, forensics, cybercrime monitoring and countermeasure development. Powered by CTU research, Dell SecureWorks' Threat Intelligence Service gives customers the early warning and actionable information needed to protect against emerging threats and vulnerabilities proactively, before they impact an organization. Service features include:

- Threat, vulnerability and advisory feeds
- Live Threat Intelligence briefings
- In-depth analysis of Microsoft Updates
- Attacker database feed
- Custom malware analysis
- Emerging Threat Bulletins
- Weekly Intelligence Summaries
- Expert support and consultation

Locations

CTP is operated out of two data centers, one in Atlanta, Georgia (GA) and the other in Lombard, Illinois (IL) while security event monitoring and device management occur at the Security Operations Centers in Atlanta, GA, Providence, RI, Lombard, IL and Myrtle Beach, SC.

The scope of this report is limited to certain Managed Security Services provided by Dell SecureWorks using the Counter Threat Platform. No other services, products or locations are within the scope of this report. Additionally, implementation of firewalls and intrusion detection systems at customer locations based on specific customer requirements is outside the scope of this report.

Relevant aspects of the control environment, risk assessment, and monitoring

Control Environment

Organizational Structure

Dell SecureWorks is organized into nine major functional groups:

- Services/Operations IT staff delivers managed security service(s) to customers in order to provide 24x7x365 protection with expertise and customer service in accordance with defined service level agreements. The Executive Director of Services/Operations IT activities at Dell SecureWorks oversees seven separate directorates: Counter Threat Platform-based Managed Security Services Delivery, ITO Security Service Delivery, Email Messaging Service/AlertFind Service Delivery, IT Operations, Dedicated Account Service Delivery, Quality-Customer Experience, and Operations Project Management. Formal organization charts indicate the functions and reporting lines at Dell SecureWorks. The hierarchical organization is conducive to control. IT operations, development and customer operations functions are organized to provide segregation of key functions with respect to development, data center support activities and customer service delivery.
- Engineering focuses on developing and deploying innovative technologies to better protect and secure customers.
- The Chief Technology Office, which includes the Counter Threat Unit™ threat intelligence research team, proactively protects customers against cyber threats around the clock. These security experts uncover emerging threats and develop countermeasures through global visibility across the customer base and insight and information exchange across many elite threat research circles.
- Sales and Marketing drives demand for security services and brand through sales, lead generation, account management, relationship building activities, public relations, sales training, market research and marketing communications.
- Product Management defines and manages the feature/functionality for innovative security products and services that meet market requirements and bring value to customers.
- Security and Risk Consulting Services, conducts consulting services on behalf of Dell SecureWorks, to include incident response & forensics, testing & assessments, compliance & certifications strategic residency services, critical infrastructure protection, and security & governance program development.
- Strategy drives security strategy alignment across other Dell, Inc. business units.
- Global Expansion leads the strategy to build a presence in strategic international markets like Asia-Pacific and Latin America.
- The Information Security Office ensures that internal security systems and processes meet stringent regulatory compliance and the demands of our customers.

Finance, Legal and HR administrative support are leveraged from Dell, Inc.

Security Management

Dell SecureWorks has established a formal security organization consisting of personnel from Risk Management and IT Operations, which, along with Corporate Information Security Committee (CISC), is responsible for setting security standards, assessing security risks, performing periodic IT security and control assessments, and facilitating security initiatives. Each functional area is responsible for the protection of systems and data under their control and carrying out the requisite security processes and procedures. Security Services Teams provide technology security direction to Dell SecureWorks products and services.

Personnel Security

Dell SecureWorks has adopted rigorous personnel security practices. Verification checks on staff are performed at the time of job application through the Dell corporate Human Resources division. Recurring background checks are performed annually for select operations personnel. Additional personnel security measures include the requirement of signed non-disclosure agreements for all Dell SecureWorks personnel and visitors to Dell SecureWorks facilities, documented job descriptions and disciplinary procedures for responding to violations.

Dell SecureWorks attempts to attract and retain highly skilled technical professionals specializing in information and network security. Background and reference checks include a consumer credit report; county/federal criminal record search; education verification (highest level completed); employment verification (most current employer only); federal criminal multi-jurisdictional record search (compilation of various database sources, includes foreign asset ownership, “world check” international crime review and sex offenses); social security number trace and address locator database.

During the application process, prospective employees are required to sign an authorization and release for a background review. As a condition of employment, employees are also required to sign a Non-Disclosure Agreement, Employee Agreement Regarding Confidentiality and Inventions as well as a User Access Agreement defining information security and physical security requirements and an acknowledgement of Dell and Dell SecureWorks’ policies.

In termination proceedings, there are at least two members of management involved with one being a member of the executive team, most often the VP of Human Resources, and the other being the employee’s supervisor. All computer and network accesses are revoked through an electronic ticketing system known as the Electronic System Resource Access/Authorization Request (eSRAAR). Company property and access cards are collected at the time of termination. Terminated employees are immediately removed from their positions once they have been discharged and physical and logical access is revoked; he or she is then escorted from the workstation and out of the building.

Risk Assessment

Dell SecureWorks has a formal risk assessment process in place to identify key risks and develop plans to address the risks uncovered during the assessment process. Dell SecureWorks management periodically performs formal security risk assessments including an Enterprise Risk Assessment and an Information Security Risk Assessment. Risks are ranked based on the impact and likelihood of potential threats. The Dell SecureWorks Board of Directors reviews the assessment on a periodic basis.

Monitoring and Compliance

The Chief Information Security Officer (CISO) Corporate Security Manager is responsible for monitoring compliance with appropriate standards, activities, regulations and industry guidelines affecting Dell SecureWorks. This is accomplished through an enterprise governance tool that assigns control standards to responsible individuals and measures the degree to which operational procedures are created and executed. Dell SecureWorks also invests in sending its employees to technical, legal, and industry conferences, meetings, and briefings. Risk Management and CISO personnel are responsible for ensuring that reports of noncompliance with security requirements are promptly addressed and that corrective measures are taken in a timely manner.

A variety of management reports are used to monitor the level of services provided to customers. Exceptions to normal or scheduled processing through hardware, software or procedural problems are logged, reported, and resolved daily. Dell SecureWorks senior management monitors the performance of each functional area by comparing it with established budgets, plans and operational benchmarks.

Information and Communication

Dell SecureWorks has internal communications procedures to help ensure that all employees understand their individual role and responsibilities concerning processing and controls. These include formal and informal orientation and training programs, the use of e-mail messages to communicate time-sensitive information, internal department websites, periodic company and department meetings, formal product team meeting minutes, reports which include a summary of follow-up items, and scripts for both security and availability purposes that notify key personnel via e-mail and pager in the event of problems. The CISO publishes a quarterly internal security awareness newsletter. Customer communication processes are defined in Service Level Agreements and customer contracts.

Information Systems – Counter Threat Platform

Dell SecureWorks' Counter Threat Platform Managed Security Services ("MSS") provide continuous monitoring of an organization's network security infrastructure. The Counter Threat Platform security monitoring tool was developed to leverage Dell SecureWorks' security intelligence and provide customers with an early warning system for Internet-based security events. In addition, Dell SecureWorks' event correlation and analysis tools enable proactive security and incident management. Dell SecureWorks provides an extension to a customer's existing network and security resources. Dell SecureWorks' MSS is built on a foundation of around-the-clock mission critical services that are rooted in Dell SecureWorks' Internet infrastructure.

Architecture Overview

The Counter Threat Platform's architecture compiles a wide range of disparate data sources and data formats from security and network devices, and converts them into a single stream of security-related events. The system then analyzes and prioritizes these events using a multi-tiered correlation process.

Dell SecureWorks' Security Operations Center (SOC) team uses Counter Threat Platform for security event monitoring and response, device management, and customer communication. Dell SecureWorks' security professionals use Counter Threat Platform on a continuous basis to:

- Identify security issues and alert customers of relevant security issues while preparing appropriate response measures, such as activating Dell SecureWorks' incident response and forensics team.
- Implement customer-directed changes to their infrastructure at any time of day, and provide ongoing management and maintenance of each customer's security technology.

Counter Threat Platform MSS customers have access to Dell SecureWorks' Customer Portal, which includes a security management dashboard where they are presented with relevant security information and reports.

Counter Threat Platform MSS Overview and Controls

Monitoring Overview

The MSS monitoring framework is based on addressing the following issues:

- Screening-out false "positive" events;
- Determining the nature of the event to determine whether the event is malicious, third party software functionality or malfunction, or unintentional end-user activity;
- In the event of a malicious event, analysis metrics are applied to attempt to ascertain what the intruder was attempting;
- Preventing attempted malicious events; and
- Preventing future malicious events.

Counter Threat Platform begins its analysis by executing focused queries against the device information that has been collected. Then, through automated analysis of these queries, the Counter Threat Platform sends applicable significant events to the SOC to initiate a review by a Security Analyst who determines if further action is needed.

Counter Threat Appliance

Counter Threat Platform Managed Security Services uses the Dell SecureWorks' Counter Threat Appliance (CTA). This device provides a communication and management channel between the customer's site and Dell SecureWorks' SOC. The CTA captures security event logs, provides an encrypted communications channel for device management and becomes an active security agent, running a variety of security protection software.

First Level Event Correlation

When acting as an event collector, the CTA captures security information from a wide range of devices, including firewalls, IDS/IDP systems, host agents, network devices, applications, and operating systems. Through a process called filtering, the CTA reduces inbound event flows to relevant security data. This data is normalized and multiple logic engines are applied to the data in order to determine the likely severity of each event. Data that passes both the normalization and logic engine steps is transferred via an encrypted tunnel to Dell SecureWorks' SOC for further analysis.

Reliability Considerations

The Dell SecureWorks' CTA also provides local data storage in order to capture all logs and data streams in the event that the Internet service is interrupted at the customer site. The CTA also provides a warm spare configuration that allows for rapid turn up of a replacement device in the case of hardware failure. Software upgrades are remotely distributed from Dell SecureWorks without requiring the customer's assistance.

Active Security Capabilities

The Dell SecureWorks' CTA is a hardened device with an active firewall configured at all times. Connectivity to and from the device is restricted to logging activities and encrypted communications to the Dell SecureWorks' Operations Center.

Data center Reliability Considerations

Counter Threat Platform is operated out of two data centers with replicated backend and redundant systems, one in Atlanta, Georgia (GA) and the other in Lombard, Illinois (IL). Dell SecureWorks has developed formal backup rotation and storage procedures. Dell SecureWorks uses Networker to back up applications and data to backup tapes. Backup schedules include daily incremental, monthly full and differential backups. If requested by management, certain critical savesets may have a more aggressive backup schedule. Backup tapes are stored locally in a fireproof container located in the Atlanta data center. Dell SecureWorks has contracted with a third party vendor to provide secure offsite storage of backup media.

Counter Threat Platform Security Operations Centers (SOC)

Counter Threat Platform security event monitoring and device management occur at the SOCs in Atlanta, GA, Providence, RI, Lombard, IL and Myrtle Beach, SC.

They are secure, highly available environments staffed on a continuous basis by security, customer care, and networking specialists. Dell SecureWorks specialists monitor the status and availability of security devices, run vulnerability scans, manage and monitor intrusion detection systems and firewalls, manage and update customers' security devices, and respond to security events.

SOC Workflow

Dell SecureWorks' SOC uses a transaction-based model for managing security events. The model relies on Counter Threat Platform's data reduction and correlation engine to keep and distribute the events created by the system at a manageable level.

With Counter Threat Platform's transaction-based approach, security events automatically generate a prioritized event populated with relevant supporting information. The trouble ticket is then queued for handling by a MSS security analyst who takes ownership of the ticket and works with the customer to resolve the issue until completion. Customers may also report issues by submitting tickets using a web-based interface called Customer Portal. During the ticket handling process, the analyst may access information stored in the Counter Threat Platform system, including log information from customer devices, or may use Counter Threat Platform's threat intelligence information to determine whether the problem exists with other client systems or other geographies.

Based on the prioritization of the security event and the review of the trouble ticket by a security analyst, MSS initiates an appropriate response that may include blocking the attack, generating a report for the MSS customer to review on the Customer Portal, or contacting the customer for live support and to discuss proper response and remediation. In the event of a major incident, MSS will engage its incident response and forensics team, preserving data and evidence for use in the legal arena. MSS will further help the customer contain and recover from the problem.

Dell SecureWorks' Customer Portal

Dell SecureWorks' Customer Portal is included in the Counter Threat Platform architecture and a primary point of contact for customer service and trouble ticketing. While providing access to near real-time security event reporting, the Customer Portal also presents timely security intelligence updates and a customized vulnerability management platform.

Dell SecureWorks' Customer Portal employs SSL encryption and customers are authenticated to the Portal through the use of a combination of user account, password, and security token. The Customer Portal offers a wide range of reports, from executive summaries to in-depth technical commentary, regarding the state of each customer's security devices.

Key features of the Customer Portal include:

- Management dashboard with seven-day vulnerability, event and ticket information;
- Sophisticated reporting that includes near real-time security events, vulnerability testing results, device configuration reports and device usage reports;
- Vulnerability alert information; and
- Self-service ticketing systems, including the ability to create and modify trouble tickets.

Communications Security

Communications between Dell SecureWorks and customer sites is secured via dedicated lines or virtual private networks (VPNs). For instance, where VPNs are used, 128-bit SSL encryption is used to secure communications between Dell SecureWorks and customer sites.

Operating System Access and Network Security

System and network security is of critical importance to Dell SecureWorks and its customers. Dell SecureWorks has documented information privacy and security policies and procedures. In order to maintain a secure infrastructure, Dell SecureWorks has certain security controls in operation. These controls include processes for managing user access to critical systems and devices, formal policies for authentication and password controls, and configuration standards for firewalls. Antivirus software, Symantec LiveUpdate, is installed on users' workstations that are used to connect to production systems. Dell SecureWorks has developed a centralized access management process whereby access to Dell SecureWorks systems, including network, the Counter Threat Platform applications and underlying infrastructure has to be approved by management. Business requirements (User Stories and Bugs) for each project team are captured in the project Confluence and JIRA project tracker pages on the intranet. Administrative access to Red Hat LINUX servers is controlled through the use of sudo (a program for Unix-like computer operating systems that allows users to run programs with the security privileges of another user) and is restricted to authorized employees only. Similarly DBA access is limited to authorized employees serving as database administrators. Dell SecureWorks has also defined password controls which includes minimum length, expiration, account lockout and password history. In addition, Dell SecureWorks has implemented monitoring controls to identify potential security threats and notify Dell SecureWorks personnel via e-mail or page, based on the severity of the threat. Authorized personnel are permitted to administer production servers and network devices only by strict controls and methods, and all access is logged and validated periodically.

Physical and Environmental Security

Dell SecureWorks has implemented a variety of physical security and environmental controls to protect Dell SecureWorks and customer assets at all Dell SecureWorks locations. Production systems housed in Dell SecureWorks data centers are protected by multiple tiers of physical security. The data centers enforce individual access control, through the use of two-factor authentication including biometrics. Individuals approved for unescorted data center access are minimal and reviewed quarterly. Physical access to the data center is automatically logged. Visitors are required to sign a log, must wear a visitor badge, and must be escorted while onsite. The data center facilities are manned continuously by on-site security personnel and the premises are continuously video monitored and recorded. Multiple generators, UPS, HVAC and fire suppression systems have been implemented at both Dell SecureWorks data centers.

Operations and Change Management

Dell SecureWorks has formalized procedures for managing the Counter Threat Platform MSS production infrastructure. These procedures include:

- Monitoring system and network capacity and availability;
- Managing the process for updating and patching critical servers and network components; and
- Increasing the assurance that media containing sensitive customer data is handled and disposed of in a controlled fashion.

Dell SecureWorks has a Change Management Board that meets twice a week to discuss and approve changes to the servers and network components, including firewalls. All changes, testing and approvals are tracked using Request for Change (RFC) tickets. Development and testing systems are physically and logically separated from production systems. Access to migrate changes into production is restricted to users with DBA privileges (databases) or sudo privileges (operating systems).

Dell SecureWorks has established a base operating systems build methodology to guide the process of server installations for IT Operations technicians. IT Operations personnel utilize the Kickstart tool to install and deploy templates and software packages for the Linux servers within the organization. Kickstart build changes are approved through the standards approval process and are made in conjunction with the Standards updates.

Control Objectives and Related Controls

The control objectives specified by Dell SecureWorks and the controls that achieve those control objectives are listed in the accompanying *Description of Control Objectives, Controls, Tests and Results of Tests.*

Complementary User Entity Controls

In designing its system, Dell SecureWorks has contemplated that certain complementary controls would be implemented by user organizations to achieve certain control objectives included in this report. The complementary user entity controls are listed below with a reference to their related control objectives in *Description of Control Objectives, Controls, Tests and Results of Tests.*

Complementary user entity controls	**Related control objectives**
User organizations are responsible for ensuring information security policies and procedures are in place and followed by customer personnel.	1, 6
User organizations are responsible for authorizing access to the Dell SecureWorks Portal and for ensuring the confidentiality of any user accounts and passwords assigned to them for use with Dell SecureWorks' systems.	6
User organizations are responsible for ensuring that account passwords are unique, not shared, non guessable, comply with security best practices in regard to length and complexity and are changed on a routine basis.	6
User organizations are responsible for removing customer access to Dell SecureWorks-supported systems in a timely manner when customer users are terminated or no longer require such access.	6
User organizations are responsible for notifying Dell SecureWorks of changes in customer authorized personnel that use the Portal.	6, 10
User organizations are responsible for providing adequate physical security over Dell SecureWorks-managed devices at the device location.	3
User organizations are responsible for determining whether Dell SecureWorks' security infrastructure is appropriate for its needs and for notifying Dell SecureWorks of any requested modifications to the service.	11
User organizations are responsible for developing their own disaster recovery and business continuity plans that address their inability to access or utilize Dell SecureWorks' services	5

Complementary user entity controls	Related control objectives
User organizations are responsible for providing proper technical support of environment and equipment surrounding installation onsite at the device location.	11
User organizations are responsible for working with Dell SecureWorks onsite engineers to verify proper installation and testing of customer applications and network functionality.	11
User organizations are responsible for ensuring that firewalls and intrusion detection systems implemented by CTP MSS have been configured in accordance with specific customer requirements.	11
User organizations are responsible for providing proper and timely authorization for changes to the hardware and software that Dell SecureWorks manages.	7, 8
User organizations are responsible for approving the implementation of Dell SecureWorks-recommended operating system and software updates and patches in a timely manner.	7, 8
User organizations are responsible for maintaining escalation procedures for customer devices.	11, 12

Service Auditor's Description of Tests of Controls and Results of Tests

Section IV – Service Auditor's Description of Tests of Controls and Results of Tests

Testing Performed and Results of Tests of Entity Level Controls

In planning the nature, timing and extent of our testing of the controls specified by Dell SecureWorks, we considered the aspects of Dell SecureWorks' control environment, risk assessment processes, information and communication and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

Control objectives, controls, tests of controls and results of tests

On the pages that follow, the description of control objectives and the controls to achieve the objectives have been specified by, and are the responsibility of, Dell SecureWorks. The testing performed by Ernst & Young and the results of tests are the responsibility of the service auditor.

Information Security Governance and Management

Control Objective 1: Controls provide reasonable assurance that management direction and support for information security are provided and compliance with Dell SecureWorks' security policies and procedures is monitored.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
1.01	Dell SecureWorks has established a formal security organization consisting of personnel from Risk Management and IT Operations, which along with Corporate Information Security Committee (CISC), is responsible for setting security standards, assessing security risks, performing periodic IT security and control assessments, and facilitating security initiatives. Each functional area is responsible for the protection of systems and data under their control and carrying out the requisite security processes and procedures.	Inspected the IT Organization Chart to determine whether Dell SecureWorks has established a formal security organization consisting of personnel from Risk Management, IT Operations and CISC. No deviations noted. Inspected the Security Strategy document to determine whether it defined the responsibilities of the security organization related to setting security standards, assessing security risks, performing periodic IT security and control assessments, and facilitating security initiatives. No deviations noted. Inspected a sample of policies and standards to determine whether the security organization had developed security standards per their responsibilities. No deviations noted. Inspected the 2012 Annual Enterprise Risk Assessment and 2012 Enterprise Information Security Risk Assessment to determine whether it was completed by the security organization. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
1.02	Dell SecureWorks has an Information Security Program which has been approved by management, published and communicated to employees and defines security objectives, provides a security framework, and emphasizes the importance of security to Dell SecureWorks' business.	Inspected the Information Security Program Overview and Corporate Security Strategy to determine whether it addressed appropriate security objectives, security policies and importance of security to Dell SecureWorks. No deviations noted. Observed the Dell SecureWorks intranet to determine whether the Information Security Program was published and available to all employees. No deviations noted. Inspected the Board of Directors Meeting Minutes to determine whether the Corporate Security Strategy was approved during the annual meeting. No deviations noted.
1.03	The Risk Management organization and IT Operations personnel are responsible for maintaining and modifying Dell SecureWorks' security program, policies, standards, and procedures. Significant changes to the Information Security Policy require approval from the Board of Directors while standards are brought to the Corporate Information Security Committee for review.	Inquired of the Director of Information Security to determine whether the Dell SecureWorks' security program, policies, standards, and procedures are maintained by the Risk Management and IT Operations team (security organization) and whether all changes have to be approved by management. No deviations noted. Inquired of Director of Information Security to determine whether significant changes to the Information Security Policy require approval from the Board of Directors. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
1.04	The Director of Information Security publishes an internal security awareness newsletter on a quarterly basis.	Inspected the internal security awareness newsletter for a sample of quarters to determine whether it was published and distributed in a timely manner. No deviations noted.
1.05	Risk Management and IT Operations personnel are responsible for ensuring that reports of noncompliance with security requirements are promptly addressed and that corrective measures are taken in a timely manner.	Inquired of Director of Information Security and CISO to determine whether reports of employee noncompliance with security requirements are promptly addressed and that corrective measures are taken in a timely manner. No deviations noted. Inspected the IA Audit Manual to determine whether instances of noncompliance with security requirements arising out of various audits and reviews are tracked and escalated so that corrective measures are taken in a timely manner. No deviations noted.
1.06	Dell SecureWorks' security policies address the types of information that must be kept confidential by Dell SecureWorks and conditions under which confidential information may be disclosed. Dell SecureWorks has a data classification project for information classification and associated protective controls for information that, per the Data Classification Policy, take into account business needs for sharing or restricting information, and the business impacts associated with such needs.	Inspected the Information Classification policy to determine whether Dell SecureWorks' security policies address the types of information that must be kept confidential by Dell SecureWorks and conditions under which confidential information may be disclosed. No deviations noted. Inspected the data classification project documents to determine whether SecureWorks has undertaken a project to classify data and information accordingly to the Data Classification Policy. No deviations noted.

Personnel Controls

Control Objective 2: Dell SecureWorks maintains controls to provide reasonable assurance that personnel and hiring policies and practices are in place to support Dell SecureWorks' operations.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
2.01	Job descriptions describe the roles and responsibilities of major positions within Dell SecureWorks IT operations.	Inspected a sample of job descriptions to determine whether they documented roles and responsibilities of the position. No deviations noted.
2.02	New employees are subject to background checks at the time of job application in accordance with Dell's employment policy.	Inspected new hire documentation for a sample of new hires to determine whether background checks were completed prior to on boarding. No deviations noted.
2.03	Employees sign a confidentiality (non-disclosure and non-solicitation) agreement as part of their terms and conditions of employment.	Inspected new hire documentation for a sample of new hires to determine whether the new employees signed a confidentiality (non-disclosure and non-solicitation) agreement. No deviations noted.
2.04	A formal disciplinary process is followed for employees who have violated Dell SecureWorks security policies and procedures.	Inquired of management to determine whether a formal disciplinary process is followed for employees who have violated Dell SecureWorks security policies and procedures. No deviations noted. Inspected the Governance, Risk and Compliance eGRC platform to determine whether formal disciplinary processes are documented and security policy violation incidents are logged and tracked. No deviations noted.

Physical Security

Control Objective 3: Controls provide reasonable assurance that physical access to the Dell SecureWorks data centers and SOCs is limited to properly authorized individuals.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
3.01	Security policies and procedures to guide activities for granting, controlling and monitoring physical access to the office facilities are documented.	Inspected policies and procedures in place to determine whether they outlined the process for granting, controlling and monitoring physical access to the office facilities. No deviations noted.
3.02	Dell SecureWorks' Security Operations Centers (SOC) and data centers have been constructed such that they cannot be entered directly from the exterior of the building. The entrances to the facilities are secured via an electronic badge access system.	Observed physical access controls in place at the Dell SecureWorks SOC and data center facilities to determine whether: • Security Operations Centers (SOC) and data centers were constructed such that they could not be entered directly from the exterior. • The entrances to the facilities were secured via badge access system. No deviations noted.
3.03	A receptionist controls access to the buildings housing the data centers and SOCs during business hours and a badge and PIN is required for after-hours access. Access to the SOC and/or data centers requires two factor authentication.	Observed physical access controls in place at the Dell SecureWorks SOC and data center facilities to determine whether: • Proximity card readers and a receptionist controlled access to the buildings housing the data centers and SOCs. • A pin was required for access after-hours. • Two factor authentication was required for access to the SOC and/or data centers. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
3.04	Visitors are required to provide photo identification when signing in to gain access to the Dell SecureWorks facilities.	Observed physical access controls in place at the Dell SecureWorks SOC and data center facilities to determine whether visitors were required to provide photo identification to gain access. No deviations noted.
3.05	The technical facility is partitioned into SOC and data center. Physical access to each is provided based on job function and visitors must be escorted.	Observed physical access controls in place at the Dell SecureWorks SOC and Data Center facilities to determine whether the technical facility was partitioned into the SOC and data center. No deviations noted. Inspected access levels for a sample of terminated employees to determine whether their access to the Dell SecureWorks SOC and Data Center facilities was removed. No deviations noted. Inspected access levels for a sample of users with access to Dell SecureWorks SOC and Data Center facilities to determine whether access was appropriate given their job responsibilities. ***Deviations noted.*** 1 out of 25 users with SOC and data center badge access were terminated employees. On expanding the sample to 50 users with access to the SOC and data centers, we noted 2 additional terminated users retained access. ***Management Response:*** All access badges belonging to the terminated employees had

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
		been collected on their last dates and therefore, no unauthorized access could have occurred subsequent to the user's termination date. For 2 of the 3 employees noted above, audit logs were available to demonstrate that the access had not been used since termination date (The third badge, belonging to an intern, was a temporary badge and was reassigned following the intern's departure; therefore, there would be no by-name log association following that date). Finally, the access for all the terminated users was disabled within the system as of October 9, 2012.
3.06	Employee and trusted contractor entry and exit to the data center and SOC are recorded in an electronic audit log. Escorted employee and visitor entry and exit are recorded in a manual audit log.	Inspected logs available in the badge system to determine whether entry and exit to the data center and SOC were recorded. No deviations noted. Inspected the manual logs to determine whether escorted employee and visitor entry and exits were recorded when they visited the Dell SecureWorks facilities. No deviations noted.
3.07	Video surveillance cameras are in place to monitor and log activity within the facility that includes, but is not limited to, the following areas: • Data center • Facility entrances	Observed physical access controls in place at the Dell SecureWorks SOC and data center facilities to determine whether video surveillance cameras were in place to monitor and log activity within the facility. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
3.08	New access requests are submitted to the asset/resource owner, who approve or deny the requests.	Inspected documentation for a sample of new Data Center users to determine whether new access requests were approved. ***Deviations noted*** 1 out of a sample of 10 new badge access users did not have a documented approval for the access. ***Management Response*** The new employee was hired as a SOC Analyst, but the initial request form erroneously omitted access request to the SOC. Since the employee was required to have SOC access, the badge administrator granted the access after verbal approval and confirmation from the employee's manager.
3.09	Administrator access to add, delete, and modify badge access rights is restricted to user accounts accessible by IT Operations personnel and third-party support vendor.	Inspected the list of personnel with centralized badge administration access rights to determine whether it was restricted to authorized users. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
3.10	Access cards are collected and/or the access configuration is changed in the event of a change in employee job responsibility or termination. The Director of Security Architecture immediately directs the de-activation of lost or stolen access cards.	Inspected a sample of terminated employees to determine whether their access to the Dell SecureWorks SOC and data center facilities was removed. No deviations noted. Inspected a sample of users with access to Dell SecureWorks SOC and data center facilities to determine whether access was appropriate given their job responsibilities. ***Deviations noted.*** 1 out of 25 users with SOC and data center badge access were terminated employees. On expanding the sample to 50 users with access to the SOC and data centers, we noted 2 additional terminated users retained access. ***Management Response:*** All access badges belonging to the terminated employees had been collected on their last dates and therefore, no unauthorized access could have occurred subsequent to the user's termination date. For 2 of the 3 employees noted above, audit logs were available to demonstrate that the access had not been used since termination date (The third badge, belonging to an intern, was a temporary badge and was reassigned following the intern's departure; therefore, there would be no by-name log association following that date). Finally, the access for all the terminated users was disabled within the system as of October 9, 2012.

Environmental Security

Control Objective 4: Control activities provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
4.01	Diesel generators are in place to provide temporary power in the event of a power failure.	Observed the Dell SecureWorks facilities to determine whether diesel generators were in place to provide temporary power in the event of a power failure. No deviations noted.
4.02	Power generators configured with self-testing ability, run weekly tests to verify that they continue to function properly.	Observed the diesel generator test indicators at Dell SecureWorks facilities to determine whether weekly tests were performed for generators with self-testing ability. No deviations noted.
4.03	A third-party vendor inspects the diesel power generators to verify that each generator is functioning properly	Inspected vendor inspection reports to determine whether a third-party vendor inspected the diesel power generators on a periodic basis. No deviations noted.
4.04	The data centers are protected by fire detection and suppression controls that may include the following: • Audible and visual fire alarms • FM-200 fire suppression system • Fire and smoke detectors	Observed the data centers to determine whether fire detection and suppression systems were in place. No deviations noted.
4.05	A third party inspects fire alarms, detectors, and suppression systems on at least an annual basis. Fire extinguishers are inspected on an annual basis by a third party.	Inspected the third-party inspection report of fire detection and suppression systems and fire extinguishers to determine whether inspections were performed in a timely manner.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
		No deviations noted.
4.06	The production servers are connected to uninterruptible power supply (UPS) systems that provide temporary electricity in the event of a power outage.	Observed the Dell SecureWorks facilities to determine whether there were UPS systems in place to provide temporary electricity in the event of a power outage. No deviations noted.
4.07	A third-party vendor inspects the UPS systems on an annual basis to verify that the systems are functioning properly.	Inspected the third party vendor inspection reports at Dell SecureWorks facilities to determine whether the UPS systems were inspected on an annual basis. No deviations noted.
4.08	The data centers are equipped with dedicated air handler units.	Observed the Dell SecureWorks data centers to determine whether air handler units were in place at the data centers. No deviations noted.
4.09	A third party vendor inspects and maintains the air handler units to help verify that the systems are functioning properly.	Inspected preventive maintenance review documentation of the air handler units to determine whether reviews were performed and documented for the data center facilities. No deviations noted.
4.10	Raised flooring is in place in the data center to elevate equipment and help facilitate cooling.	Observed the Dell SecureWorks data centers to determine whether raised flooring was in place. No deviations noted.

Computer Operations Management

Control Objective 5: Control activities provide reasonable assurance that production processing systems are maintained in a manner that helps ensure system availability, and production processing systems are monitored and processing deviations are identified and resolved.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
5.01	Operating procedures are documented and maintained by the IT Operations group.	Inspected the Operating Procedures in place to determine whether the procedures were documented and made available to employees. No deviations noted.
5.02	Management maintains formal backup rotation and storage policies.	Inspected the Production Backup Standard to determine whether formal backup rotation and storage policies were in place. No deviations noted.
5.03	Backup tapes are stored locally in a fireproof container prior to being transported for offsite storage by a third party vendor.	Observed the local facilities to determine whether archival media was stored in fireproof containers prior to being transported for offsite storage by a third party vendor. No deviations noted.
5.04	IT management has contracted with a third-party vendor to provide secure offsite storage of archival media.	Inspected the Iron Mountain contract to determine whether IT management had contracted with a third party vendor to provide secure offsite storage of archival media. No deviations noted.
5.05	Database replication occurs real-time between the various sites.	Inspected the database replication configurations between various Dell SecureWorks sites to determine whether databases were replicated real time. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
5.06	A backup management tool is utilized to schedule and monitor backups on a daily basis. Errors are investigated and resolved.	Inspected the configuration within the Networker backup job scheduler to determine whether the backups were scheduled to run on a daily basis. No deviations noted. Inspected the configuration within the Networker backup system and the notification email to determine whether the system is configured to automatically notify appropriate personnel of backup failures. No deviations noted. Inspected a sample of backup logs to determine whether configured backups ran as scheduled and errors, if any, were resolved. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
5.07	Computer operations personnel have configured the automated backup systems to perform backups on the following basis: • Daily incremental backups • Full backups once a month • Differential backups on weekends that full backups are not performed • Nightly CTP database backups	Inspected the configuration within the Networker backup job scheduler to determine whether the backups were scheduled to run: • Daily incremental backups • Full backups once a month • Differential backups on weekends that full backups are not performed • Nightly CTP database backups No deviations noted. Inspected a sample of backup logs to determine whether configured backups ran as scheduled and errors, if any, were resolved. No deviations noted.
5.08	Due to the criticality of the data or the need to reduce the time-to-recover, either Management or Architecture may request an enhanced policy be implemented for certain savesets. In these cases backups will be performed on the following basis: • Full backups once per week • Nightly incremental backups.	Inspected the configuration within the Networker backup job scheduler to determine whether the backups were scheduled to run: • Full backups once per week on critical savesets. • Nightly incremental backups on critical savesets. No deviations noted. Inspected a sample of backup logs to determine whether configured backups ran as scheduled and errors, if any, were resolved. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
5.09	IT Operations are required to use a ticketing system to record and monitor operational problems.	Inquired of the Network Support Manager to determine whether a ticketing system is used to record and monitor operational problems. No deviations noted. Inspected a sample of tickets to determine whether IT Operations used a ticketing system to record and monitor operational problems. No deviations noted.
5.10	Tickets are submitted into the system via e-mail and via web interface. Each ticket can be updated by the submitter or the operator multiple times, and a record of correspondence and notes is maintained. Tickets are assigned to individual analysts and may also be placed in multiple queues to organize their resolution.	Observed the ticketing system to determine whether tickets were submitted into the system via e-mail and via web interface. No deviations noted. Inspected a sample of tickets to determine whether: • Tickets were updated by submitters or operators; • Tickets were assigned to the analysts to resolve the issue; and • Notes were maintained to indicate resolution or related correspondence. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
5.11	The IT Operations team actively monitors the availability and operational status of Dell SecureWorks systems.	Inquired of the Network Support Manager to determine whether the IT Operations team actively monitors the availability and operational status of Dell SecureWorks system. No deviations noted. Inspected a sample of help desk tickets to determine whether IT Operations monitored the availability and operational status of Dell SecureWorks systems. No deviations noted. Observed the monitoring screens in the SOC to determine whether MSS personnel were automatically notified of critical security events. No deviations noted.
5.12	The IT Operations personnel are notified when predefined thresholds are exceeded on monitored network devices.	Inspected a sample of tickets to determine whether IT Operations used a ticketing system to record, assign, and notify IT Operations of operational incidents. No deviations noted. Observed the monitoring screens in the SOC to determine whether MSS personnel were automatically notified of critical security events. No deviations noted.

System Access Management and Network Security

Control Objective 6: Controls provide reasonable assurance that MSS system access is limited to properly authorized individuals and production network access is limited to properly authorized individuals, systems and services.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
6.01	Management maintains documented information privacy and security policies and procedures.	Inspected policies and procedures in place to determine whether they included information privacy and security policies and procedures. No deviations noted.
6.02	Administrative access to the Dell SecureWorks network is restricted to authorized personnel.	Inspected access levels of all the users with administrative access to the network domain to determine whether it was restricted to the appropriate employees. No deviations noted.
6.03	Access to information systems is assigned by job responsibility via a centralized access management process that includes management and / or security approval.	Inspected documentation for a sample of new users to determine whether their access was approved via a centralized access management process that included management and/or security approval. ***Deviations noted*** 2 new users out of a sampie of 25 did not have documented approvals. ***Management's Response*** Although the centralized access management process was not followed for the two users, the access was authorized by the members' management, executed through proper ticketing and appropriate for their job functions.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
6.04	IT Operations personnel revoke terminated employees' access to their assigned system user accounts upon notification of employee termination.	Inspected access rights for a sample of terminated users/hires to determine whether their access to the network and the CTP systems were revoked. ***Deviations noted.*** 4 out of a sample of 12 terminated employees continued to have access to the CTP Systems. ***Management's Response:*** For 3 out of the 4 deviations, the terminated user's network access had been deleted, which is required prior to authenticating to the CTP system and for the 4th terminated user, the network access had not been used since termination date. Because of the layered access protections in use, the user would first need to authenticate to Active Directory in order to gain access to privileged resources. The network and CTP system access for all 4 users has been deleted as of October 2012.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
6.05	Active directory is configured to enforce the following user account and password controls: • Minimum password length - 8 • Complexity requirements – enabled • Minimum password history – 7 • Password expiration intervals – 72 days • Invalid password account lockout threshold – 3 failed attempts for 30 minutes • Store password using reversible encryption disabled • Minimum password change – 14 days	Inspected the active directory password policies to determine whether the following password controls were in place: • Minimum password length – 8 • Complexity requirements – enabled • Minimum password history – 7 • Password expiration intervals – 72 days • Invalid password account lockout threshold – 3 failed attempts for 30 minutes • Store password using reversible encryption disabled • Minimum password age – 14 days No deviations noted.
6.06	LDAP is configured to enforce the following user account and password controls: • Minimum password length – 7 • Minimum password history – 6 • Complexity requirements – choice of 3 • Password expiration intervals – 72 days • Invalid password account lockout threshold – 3 failed attempts • Minimum password change – 14 days	Inspected the LDAP password configuration settings to determine whether the following password controls were in place: • Minimum password length – 7 • Minimum password history – 6 • Complexity requirements – choice of 3 • Password expiration intervals – 72 days • Invalid password account lockout threshold – 3 failed attempts • Minimum password change – 14 days No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
6.07	Network and system vulnerability scans are run weekly. Management reviews vulnerability scan results and issues are remediated as defined in Dell SecureWorks standards.	Inspected the vulnerability dashboard for a sample of weeks to determine whether network and system vulnerability scans were run weekly. No deviations noted. Inquired of the Manager of the Corporate Incident Response Team to determine whether vulnerability scan issues were remediated as defined in Dell SecureWorks standards. No deviations noted. Inspected the vulnerability dashboard to determine whether vulnerability scan resolution remediation was tracked by risk level, as defined in Dell SecureWorks standards. No deviations noted.
6.08	Administrative access to LDAP is restricted to user accounts accessible by the appropriate IT Operations personnel.	Inspected administrative access to LDAP to determine whether the access was restricted to appropriate personnel. No deviations noted.
6.09	Administrative access to the LINUX operating systems is restricted to user accounts accessible by the appropriate IT personnel.	Inspected the access rights for a sample of users with administrative access to the LINUX operating system to determine whether it was restricted to the appropriate personnel. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
6.10	Administrative access to the CTP Portal is restricted to the appropriate IT personnel.	Inspected access rights of all users with administrative access to the Portal to determine whether the access was restricted to the appropriate IT personnel. No deviations noted.
6.11	Server audit logs are encrypted. Access to the logs is restricted to user accounts accessible by the appropriate IT personnel.	Inspected the authentication process for LogVault within the CTP portal to determine whether a valid certificate was required when authenticating to the Portal to access the logs. No deviations noted. Inspected the log repository to determine whether audit logs stored within were encrypted. No deviations noted. Inspected a sample of users' access to the LogVault logs to determine whether access was restricted appropriately. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
6.12	Database administration rights are restricted to user accounts accessible by the appropriate IT personnel.	Inspected access rights of all users with DBA privileges to determine whether access was restricted to appropriate personnel. ***Deviations Noted*** 2 out of a total population of 14 user accounts with DBA privileges belonged to terminated users. ***Management Response*** Access to the DB cannot occur unless the user is first authenticated to the network. Because credentials had been surrendered, access to workstations and authentication to the DB was not possible. The terminated users' accounts had not been used since the termination date. Additionally, the access was removed as of October, 2012.
6.13	Customers are authenticated to the Portal through the use of one of the following methods: • Digital certificate • Combination of user account, PIN, and security token	Observed an attempt to login to the Portal to determine whether customers were authenticated to the Portal through the use of one of the following methods: • Digital certificate • Combination of user account, PIN, and security token No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
6.14	Access to the CTP applications requires a user account with a password protected certificate for authentication. The password must be at least 8 characters and contain at least one upper case letter, one lower case letter, and one special character.	Observed an attempt to login to the portal to determine whether Dell SecureWorks employees required a digital certificate and password to authenticate. No deviations noted. Observed an attempt to create a new certificate password to determine whether the system required a password of at least eight characters, at least one upper case letter, one lower case letter, and one special character. No deviations noted.

System Development

Control Objective 7: Controls provide reasonable assurance that systems development activities are properly controlled, approved, and authorized.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
7.01	Dell SecureWorks maintains a documented software development methodology to guide employees in reviewing and understanding requirements and delivering the appropriate application changes through proper construction, testing, and delivery to Tech Ops for implementation.	Inspected the SDLC Methodology to determine whether the policy guided employees in reviewing and understanding requirements and delivering the appropriate application changes through proper construction, testing, and deliver to Tech Ops for implementation. No deviations noted.
	Dell SecureWorks business requirements are captured in project development proposals (PDP) and are given a level of effort and a stack rank.	Inspected documentation for a sample of projects to determine whether business requirements were captured in PDPs and were ranked by level of effort. No deviations noted.
	Business requirements (User Stories and Bugs) for each project team are captured in the project Confluence page.	Observed the Confluence intranet web pages to determine whether business requirements (User Stories and Bugs) for each project team were captured within. No deviations noted.
7.02	Dell SecureWorks tracks the development of new features and bug fixes using a single internal planning and tracking system.	Inspected documentation for a sample of projects to determine whether development of new features and bug fixes was tracked using the Confluence and JIRA tracking tools. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
7.03	Dell SecureWorks maintains a Change Management Board to review and approve changes.	Inspected documentation for a sample of projects to determine whether the Change Management Board reviewed and approved the changes. No deviations noted.
7.04	Access to migrate a release to production is restricted to the appropriate IT personnel. Logical access to the code versioning system is limited to authorized personnel.	Inspected a listing of all users with access to sudo to determine whether access was limited to authorized personnel. No deviations noted. Inspected a listing of all users with access to RedHat Satellite code migration tool to determine whether access was limited to authorized personnel. No deviations noted. Inspected a sample of users from a listing of subversion code versioning tool users to determine whether access was limited to authorized personnel. ***Deviations noted.*** 3 out of a sample of 42 employees with access to the subversion code versioning tool were terminated employees. ***Management Response*** Access to the subversion system is only possible through authentication to the network. Audit logs demonstrated that the terminated users' accounts had not been used since the termination date and therefore access to subversion was not possible. Additionally, the access was removed as of October, 2012.

System Change Control

Control Objective 8: Controls provide reasonable assurance that unauthorized changes are not made to networks, servers, and operating systems.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
8.01	The ability to migrate system software changes is restricted to user accounts accessible by IT Operations administrators and directors.	Inspected a list of all users with privileged access to LINUX to determine whether the access were appropriate given their job responsibilities. No deviations noted. Inspected a listing of all users with access to RedHat Satellite code migration tool to determine whether access was limited to authorized personnel. ***Deviations noted.*** 2 user accounts out of a total population of 28 users had inappropriate access to make changes to the production environment via use of the RedHat Satellite tool. ***Management Response*** The user accounts were previously appropriate but are no longer required. The user accounts have not been used during the reporting period and have been deleted as of October 2012. Inspected a sample of users from a listing of subversion code versioning tool users to determine whether access was limited to authorized personnel. ***Deviations noted.*** 3 out of a sample of 42 employees with access to the

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
		subversion code versioning tool were terminated employees. ***Management Response*** Access to the subversion system is only possible through authentication to the network. Audit logs demonstrated that the terminated users' accounts had not been used since the termination date and therefore access to subversion was not possible. Additionally, the access was removed as of October 2012.
8.02	The Change Management Board meets on a semi-weekly basis to schedule and prioritize software releases and system changes. Security patch levels are also maintained in this manner.	Inquired of Project Program Management Sr. Advisor to determine whether the Change Management Board met on a semi-weekly basis to schedule and prioritize software releases and system changes. No deviations noted. Inspected meeting minutes for a sample of weeks to determine whether the Change Management Board met on a semi- weekly basis to schedule and prioritize software releases, system changes and security patches. No deviations noted.
8.03	System software changes must be approved by the Change Management Board prior to being migrated into the production environment.	Inspected documentation for a sample of system software changes to determine whether they were approved by the Change Management Board prior to being migrated into the production environment. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
8.04	IT Operations personnel utilize a ticket tracking system to document and maintain scheduled and emergency changes to system software.	Inspected documentation for a sample of system software changes to determine whether a ticketing system was used to track testing and approval of all changes. No deviations noted.
8.05	Outages of critical operations components are recorded using tickets. Severity 2 and higher outages are put through Root Cause Analysis (RCA) Process. RCA results are available within 5 business days of the outage.	Inspected documentation for a sample of Severity 2 or higher system outages to determine whether outages of critical operations components were documented in a Root Cause Analysis (RCA) and distributed within 5 business days of the outage. No deviations noted
8.06	System software change implementation dates are logged within the change ticketing tool and emailed to certain personnel.	Observed the change ticketing tool to determine whether system software changes schedules were posted. No deviations noted Inspected emails for a sample of weeks to determine whether system software change details and schedules were e-mailed to the Change Management team members. No deviations noted.
8.07	A base operating systems build methodology is documented to guide the process of server installations for IT Operations technicians.	Inspected the base operating system build methodology document to determine whether it was documented to guide the process of server installations for IT Operations technicians. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
8.08	IT Operations personnel utilize the Kickstart tool to install and deploy templates and software packages for the Linux servers within the organization.	Inspected a report from the Kickstart tool to determine whether the Kickstart tool was used to install and deploy templates and software packages for the Linux servers within the organization. No deviations noted. Inspected a sample of CTP production servers deployed during this audit period to determine whether they were initialized and configured using the Kickstart system tool. No deviations noted.
8.09	Kickstart build changes are approved through the standards process and are made in conjunction with Standards updates.	Inspected the base operating system methodology document and inquired of the Systems Administration Manager to determine whether Kickstart build changes were approved through the standards process and were made in conjunction with Standards updates. No deviations noted.

Data Communications

Control Objective 9: Controls provide reasonable assurance that integrity and security of data is maintained as it is transmitted between Dell SecureWorks and its MSS customers.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
9.01	Intrusion Detection System (IDS) devices are configured to submit health and wellness information (EKG) at least once every five minutes.	Inspected IDS device monitoring log for a sample of devices to determine whether devices sent health and wellness information (EKG) at least once every five minutes. No deviations noted.
9.02	IDS devices are configured to send an alert to the SOC via an EKG flat-line ticket in the event an EKG is not received for a pre-defined period.	Observed the monitoring processes in place within the CTP portal and at the SOC to determine whether IDS devices were configured to send an alert to the SOC in the event an EKG was not received for a pre-defined period. No deviations noted. Observed the event viewer in the SOC to determine whether SOC analysts were notified of security events. No deviations noted. Inspected a sample of tickets to determine whether SOC followed the documented escalation procedures to contact the client regarding the availability issue and resolve it in a timely manner. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
9.03	SOC personnel troubleshoot and notify the customer contact of device availability issues.	Observed operations in the SOC to determine whether clients were contacted in the event of an issue. No deviations noted. Inspected a sample of Remedy tickets to determine whether clients were notified of device failure. No deviations noted.
9.04	The SOC communicates with customer devices via encrypted Secure Socket Layer (SSL) sessions.	Inquired of the Network Security Sr. Advisor to determine whether the SOC communicated with client devices via encrypted Secure Socket Layer (SSL) sessions. No deviations noted Inspected communications between the SOC and a sample of client devices to determine whether the SOC communicated with client devices via encrypted Secure Socket Layer (SSL) sessions. No deviations noted
9.05	The iSensor agents are configured to accept commands from pre-defined Dell SecureWorks Internet Protocol (IP) address space. These agents only communicate via specifically assigned ports. Once authorized communication is established, and confirmed via digital certificate validation, the iSensors can accept commands from the SOC.	Inquired of the Solutions Architect Consultant to determine whether iSensor agents were configured to accept commands from pre-defined Dell SecureWorks Internet Protocol (IP) address space. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
		Inquired of the Solutions Architect Consultant to determine whether a security build script was used to configure iSensor agent servers to accept commands from pre-defined Dell SecureWorks Internet Protocol (IP) address space. No deviations noted. Inspected the security build script to determine whether it included configuration of iSensor agent servers to accept commands from pre-defined Dell SecureWorks Internet Protocol (IP) address space. No deviations noted. Inspected configuration for a sample of client iSensor devices to determine whether it was configured to accept commands from pre-defined Dell SecureWorks Internet Protocol (IP) address space. No deviations noted.
9.06	Emails sent from the SOC to customers are automatically digitally signed (for customers that have requested this option within the Portal), so that they may validate the source of the email.	Inspected the portal configuration and an email for a sample of clients to determine whether emails between SOC and clients can be configured to be digitally signed. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
9.07	iSensors are assigned a unique device specific identifier that is utilized for communication.	Inquired of the Business Systems Consultant to determine whether iSensor devices were automatically assigned a unique device specific identifier by the CTP application utilized for communication. No deviations noted. Inspected configuration details of a device to determine whether it was assigned a unique identifier. No deviations noted. Inspected a listing of all client devices to determine whether each iSensor devices was assigned a unique device specific identifier. No deviations noted.
9.08	A firewall system is in place to filter unauthorized inbound network traffic from the Internet.	Inspected network diagrams to determine whether firewall systems were in place to filter unauthorized inbound network traffic from the Internet. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
9.09	The firewall system is configured to allow only specific services to specific destinations and deny undefined traffic.	Inquired of the Network Security Manager to determine whether deny-all rules were configured on all corporate firewalls for unauthorized incoming network traffic. No deviations noted. Inspected a sample of firewall rules to determine whether these rules were configured to allow only specific services to specific destinations and deny undefined traffic. No deviations noted.
9.10	Access to modify the firewall system configurations or rules sets is restricted to user accounts accessible by the appropriate IT Operations personnel.	Inspected access rights for a sample of users, to determine whether access to modify firewall system configurations or rule sets were limited to appropriate IT Operations personnel. No deviations noted.
9.11	Inbound Internet traffic terminates at a host in the demilitarized zone (DMZ) which is separate from the local area network (LAN) at the Dell SecureWorks facilities.	Inquired of the Network Security Manager to determine whether demilitarized zones were in place to terminate inbound Internet traffic sent to Dell SecureWorks. No deviations noted. Inspected the network diagrams to determine whether demilitarized zones were in place to terminate inbound Internet traffic sent to Dell SecureWorks. No deviations noted.

Portal User Account Maintenance

Control Objective 10: Controls provide reasonable assurance that user accounts are authorized and provisioned to the Managed Security Services' Portal and on a per customer basis.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
10.01	Management maintains formal procedures to guide SOC personnel in performing Customer Verification Procedures.	Inspected the Client Verification Procedures to determine whether formal procedures were documented to guide SOC personnel in performing client verification procedures. No deviations noted. Observed CTP systems to determine whether the Client Verification Procedures were available within the system for easy access and whether appropriate information was available to the SOC personnel to perform verification procedures. No deviations noted.
10.02	Only customers who provide valid security credentials (a Portal user account and token) can access the Dell SecureWorks Portal.	Observed the Portal to determine whether customers' accounts could be accessed only with valid security credentials. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
10.03	A ticketing system is utilized to track the addition, modification, or deletion of customer access requests.	Inquired of the Network Security Manager to determine whether clients have access to add, modify or delete portal accounts for themselves. No deviations noted. Inquired of the Network Security Manager to determine whether a ticketing system is used to track addition, modification or deletion of client access requests. No deviations noted. Inspected documentation for a sample of client access requests to determine whether they were tracked using a ticketing system. No deviations noted.
10.04	Customers are authenticated to the Portal through the use of one of the following methods: • Digital certificate • Combination of email, password and security token	Observed an attempt to login to the Portal to determine whether clients are authenticated to the Portal through the use of one of the following methods: • Digital certificate • Combination of email, password and security token No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
10.05	Digital certificates are created with a complex password that is determined by Dell SecureWorks.	Observed the new certificate generation wizard to determine whether passwords were required prior to certificate creation for CTP customers. No deviations noted. Observed an attempt to create a new certificate password to determine whether the system required a password of at least eight characters, at least one upper case letter, one lower case letter, and one special character. No deviations noted.
10.06	Customer Portal utilizes 256 bit advanced encryption standard (AES).	Inspected the Portal configuration to determine whether it utilized 256 bit advanced encryption standard (AES). No deviations noted.
10.07	Customers accessing the Portal from their facilities are restricted to only their data.	Observed the Portal for a sample of clients to determine whether access to the Portal is segregated by client. No deviations noted. Inspected Portal configuration settings for a sample of customers, to determine whether access to data through the Dell SecureWorks Portal is segregated by customer. No deviations noted. Inquired of management to determine whether clients can choose to allow their employees to have access to security event and device data by service or devices. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
10.08	Super user privileges to the Portal are restricted to managers or their designated representatives within Device Management, SOC and Operational Intelligence. In addition, a limited number of Quality Assurance engineers may be allowed access to aid in portal testing and system functionality.	Inspected access rights of all users with administrative access to the Portal to determine whether the access was restricted to the appropriate employees as noted in the control. No deviations noted.

Customer Premise Equipment (CPE)/Customer Systems Management

Control Objective 11: Controls provide reasonable assurance that communications links between Dell SecureWorks and MSS customer locations are secured and monitored.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
11.01	Communications links between Dell SecureWorks and MSS customer locations are via secured connections.	Inspected the communications log between Dell SecureWorks and clients to determine whether the communication occurred via secured connections. No deviations noted. Inspected the connection between Dell SecureWorks and a device at a customer location to determine it was through a secured connection. No deviations noted.
11.02	Communications between Dell SecureWorks and MSS customer locations over public networks are encrypted.	Inquired of management to determine whether communications between Dell SecureWorks and MSS customer locations over public networks are encrypted. No deviations noted. Inspected email communications between customer and Dell SecureWorks to determine whether it was encrypted. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
11.03	Dell SecureWorks continuously monitors the availability of its connections with customer locations. An event is automatically generated if a Dell SecureWorks managed device connection becomes unavailable.	Inspected IDS settings to determine whether devices sent health and wellness information (EKG) at least once every five minutes. No deviations noted. Observed the monitoring processes in place within the CTP portal and at the SOC to determine whether IDS devices were configured to send an alert to the SOC in the event an EKG was not received for a pre-defined period. No deviations noted. Observed event viewer in the SOC to determine whether SOC analysts were notified of security events. No deviations noted. Observed the monitoring screens in the SOC to determine whether MSS personnel were automatically notified of critical security events. No deviations noted.

Customer Issue Resolution

Control Objective 12: Controls provide reasonable assurance that alerts and incidents are resolved completely, timely and in accordance with customer service agreements.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
12.01	Documented procedures are in place to guide personnel in responding to, escalating, and resolving customer issues.	Inspected the SOC escalation policies and procedures to determine whether the escalation procedures were documented and made available to the SOC. No deviations noted. Inspected the 'Escalating an Event Procedure' followed by SOC personnel when addressing and escalating an issue to determine whether these procedures were documented. No deviations noted. Inspected a sample of tickets to determine whether the SOC followed the documented escalation procedures to contact the client regarding the availability issue and resolve it in a timely manner. No deviations noted.
12.02	The SOC is staffed by operations personnel 24 hours a day.	Inspected the ticketing system to determine whether tickets were logged and addressed 24 hours a day. No deviations noted. Inspected the SOC schedule to determine whether personnel were scheduled to be on-site 24 hours a day. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
12.03	SOC analysts are notified of security events via the event viewer.	Observed the event viewer in the SOC to determine whether SOC analysts were notified of security events. No deviations noted. Observed the monitoring screens in the SOC to determine whether MSS personnel were automatically notified of critical security events. No deviations noted.
12.04	The SOC technician desks are equipped with alarms used to alert them of the most critical security events.	Observed the SOC facilities to determine whether the SOC technician desks are equipped with alarms used to alert them of the most critical security events. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
12.05	SecureWorks continuously monitors the availability of its connections with managed devices at customer locations. An alert ticket is automatically generated if a SecureWorks managed device connection becomes unavailable.	Observed the event viewer in the SOC to determine whether SOC analysts were notified of security events. No deviations noted. Inspected the ticketing system to determine whether tickets were logged and addressed 24 hours a day. No deviations noted. Observed the SOC schedule to determine whether personnel were scheduled to be on-site 24 hours a day. No deviations noted. Inspected a sample of Remedy tickets to determine whether a ticket was generated and sent to the SOC queue when device connections became unavailable. No deviations noted.
12.06	Audible and visual alerts are utilized to notify SOC personnel of tickets in queue.	Observed activities in the SOC to determine whether SOC analysts were notified of security events via audible and visual alerts. No deviations noted.
12.07	A color-coded situational display is utilized to track and monitor events and incidents.	Observed activities in the SOC to determine whether a color-coded situational display was utilized to track and monitor events and incidents. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
12.08	An escalation procedure is utilized for customer devices to help increase the assurance that customers are notified of security events.	Observed the use of escalation policies and procedures within the SOC to determine whether the escalation policies and procedures were followed. No deviations noted. Inspected a sample of tickets to determine whether SOC followed the documented escalation procedures to contact the customer regarding the availability issue and resolve it in a timely manner. No deviations noted.
12.09	IT management maintains an escalation contact list to minimize disruptions in operations processing.	Inspected the escalation contact list in place to determine whether personnel were identified to address event escalation and minimize disruptions. No deviations noted.
12.10	Dell SecureWorks tracks customer-requested change requests by creating tickets in the Portal system.	Inspected documentation for a sample of change requests to determine whether the changes were tracked in a Remedy ticket and completed. No deviations noted.

#	Key Controls Specified by Dell SecureWorks	Testing Performed and Results of Tests
12.11	SOC personnel acknowledge security incidents within 15 minutes of ticket submission.	Observed event viewer in the SOC to determine whether SOC analysts were notified of security events. No deviations noted. Observed the event viewer in the SOC to determine whether events had been acknowledged within 15 minutes of ticket submission. No deviations noted. Inquired of management to determine whether SOC analysts acknowledged events within 15 minutes of ticket submission. No deviations noted. Inspected a sample of security incidents to determine whether SOC analysts acknowledged events within 15 minutes of ticket creation. No deviations noted.

Other Information Provided by Dell

The information in this section is presented by management of Dell SecureWorks to provide additional information and is not part of Dell SecureWorks' Description that may be relevant to a user organization's internal control. Such information has not been subjected to the procedures applied in the examination of the Description applicable to Dell SecureWorks and, accordingly we express no opinion on it.

Section V – Other Information Provided by Dell

Dell SecureWorks believes that control deviations discovered during the SSAE16 audit do not pose systemic weakness and, in the view of the company, suggest no proximate threat or vulnerability. Layered defenses, to include privileged access restrictions through Active Directory as well as two-factor remote authentication requiring the SecurID token, prevented any terminated employees from gaining any unauthorized access. Additionally, the Electronic System/Resource Authorization Access Request (eSRAAR) has added unprecedented discipline to granting and revoking privileged accesses during onboarding and termination, yet very limited instances may occur where accesses are granted by management (through appropriate ticketing) outside the process. Dell SecureWorks is bolstering awareness among all personnel on the use of eSRAAR and maintaining vigilance in ensuring only valid privileges are assigned and retained through twice-annual access reviews known as iAttest. Moreover, unauthorized physical access was not possible as badges had been revoked at the time of departure, and audit logs showed no attempted accesses by registered badge holders. There is a quarterly review standard in place for physical access to sensitive computing facilities which CISO oversees.

Appendix A – Subservice Organizations

Appendix A – Subservice Organizations

Dell SecureWorks uses the following subservice organizations to provide certain services. The control objectives and controls of these subservice organizations are outside the scope of this report.

Iron Mountain provides archival tapes storage services.

Prime Power has been contracted to service the Atlanta, GA location diesel generators.

Patton Power Systems has been contracted to service the Lombard, IL location diesel generators.

Carolina Temperature Control, Inc.'s Power Systems Group has been contracted to service the Myrtle Beach, SC location diesel generator.

Schneider Electric has been contracted to inspect and service the Atlanta, GA and Lombard, IL UPS systems.

Certified Fire Protection, Inc. provides inspection and maintenance services for the Atlanta, GA location fire alarms and suppression systems.

Affiliated Customer Service, Inc. provides inspection and maintenance services for the Lombard, IL location fire alarms and suppression systems.

Security Vision has been contracted to inspect and service the Myrtle Beach, SC fire suppression system.

Pye Barker Consulting Company has been contracted to inspect and service the Myrtle Beach, SC fire extinguishers.

McKenney's Mechanical Contractors and Engineers provides HVAC inspection and maintenance services for the Atlanta, GA location.

AMS Mechanical Systems, Inc. provides HVAC inspection and maintenance services for the Lombard, IL location.

Red Flag Oversight Policies

Southeastern Data Cooperative

October 10, 2008

SEDC
Southeastern Data Cooperative

Southeastern Data Cooperative, Inc.
2100 East Exchange Place, Suite 300, Tucker, GA 30084-5313

SEDC
Southeastern Data Cooperative

Red Flag Service Provider Oversight

Introduction

The Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) have issued regulations (the Red Flag Rules) requiring financial institutions and creditors to develop and implement written identity theft prevention programs, as part of the Fair and Accurate Credit Transaction (FACT) Act of 2003. The programs must be in place by November 1, 2008 and must provide for the identification, detection, and response to patterns, practices, or specific activities – known as "red flags" – that could indicate identity theft.

Critical to the aforementioned regulation is that a *"Creditor – Utility Company"*, which falls squarely within the scope of the regulation, must exercise appropriate and effective oversight of their *"Service Provider."* Since SEDC, along with its subsidiaries, is the *"Service Provider"* for its utility customers, it is the intent of SEDC to satisfy the utility companies' oversight requirement in a manner that does not jeopardize the current service levels SEDC's customers have come to expect.

This document provides high level descriptions of the various internal controls and policies that exist within SEDC relating to securing SEDC's customer data.

Acknowledgment and Receipt of Identity Theft Policy

All employees of SEDC and its subsidiaries are required to read and sign the "Acknowledgement and Receipt of Identity Theft Policy" as a condition of employment. The purpose of the Identify Theft Policy is to raise awareness of the importance SEDC places on the security of customer data and the consequences of violating the Identity Theft Policy (See Page 5).

Customer Support

As part of the Identity Theft Policy mentioned above, NO SEDC employees, including those in support roles, are to access any parts of the utility's system without express permission by the utility. These "parts" of a utility's system include but are not limited to their network, servers on their network, databases located on those servers, and stored databases located at SEDC's physical location for utilities utilizing the Disaster Recovery service. Employees in violation of this policy are subject to removal from their current position, including dismissal. Employees are required to sign the Acknowledgment and Receipt of Identity Theft Policy which provides explicit details of the policy.

Key points of this policy primarily directed at support personnel are as follows:

- Access into customer's systems, which includes a customer's database residing in the SEDC facility, is strictly prohibited unless permission has been given by the customer to access those systems and or database(s).

- Personal information from a customer's system is not to be downloaded, copied, or otherwise retrieved, if at all possible.

- The customer will be notified of the information retrieved, if it does become necessary to download, copy, or retrieve personal information stored on a customer's system.

- Under NO CIRCUMSTANCE will personal information stored on a customer's system be distributed to any third party without the written consent of the customer's management.

- Personal information that is appropriately retrieved from a customer's system will be placed in a secure location at the end of each working day.

- Personal information that is appropriately retrieved from a customer's system and printed will be shredded once its useful life has expired.

- The duty of all managers, supervisors, and employees is to ensure that the above points are adhered to and monitored through observations and proprietary reporting systems. Violations from the above points are to be escalated to any and all senior management including the CEO.

In addition, the management of SEDC will notify customers of the nature and extent of a breach when it appears that such a breach is of a fraudulent nature.

While SEDC recognizes the seriousness of Identity Theft, SEDC intends to apply a prudent approach in the application of the above policy such that service levels to our customers are not jeopardized.

Exceptions to The Above

As a matter of practicality, certain exceptions ***do apply*** to the first item in the above policy,

> *"Access into customer's systems, which includes a customer's database residing in the SEDC facility, is strictly prohibited unless permission has been given by the customer to access those systems and or database(s).*

These exceptions can be characterized as a single core foundational value which has been instrumental in SEDC's thirty-two year success story. This foundational value is to *serve the* *customer*. Certain products and services provided to our community of utilities have become an extension of those utilities' operations. Hence, requiring authorization on a minute by minute basis for certain types of services and functions provided by SEDC is simply impractical.

For example, customers utilizing Disaster Recovery have agreed in the contract that *"The customer will provide SEDC secure access to the customer's data as specified by SEDC for database and log transfer."* Similarly, customers provided the various financial service services have agreed to allow automated processes as well as manual processes on a 24/7 basis in achieving a reliable, efficient and effective payment processing service. These are just two real-time examples of processes actively engaged in your system as you read this document.

Disaster Recovery (DR)

The disaster recovery service is structured to ensure the highest possible security level within an acceptable cost structure that ensures a prudent, efficient and effective solution to a utility's disaster recovery needs.

The security attributes associated with the DR system are as follows:

- No open ports exist into the DR server firewall from the outside.
- The network is isolated with 100% segmentation.
- Customers' databases are stored on a dedicated, privately maintained HP 9000 server.
- Access to the system is restricted to two Oracle DBAs and one Unix System Administrator, all of whom are employed by SEDC.
- Access is restricted to a total of three IP addresses for the PCs assigned to the DBAs and Unix System Administrator.
- Data is transmitted from the utilities to SEDC using UNIX's Secured Shell Protocol (SSH). This secures the transmission of data using Best Practices encryption technology.
- Databases are backed up to tape nightly and stored in a secure room.
- Tape backups are also stored at a secured offsite storage vendor on a weekly basis.
- This system is monitored daily between the two Oracle DBAs and the Unix System Administrator to ensure the system maintains the highest level of security and reliability possible.

Financial Services

The financial services department of SEDC is comprised primarily of bill payment services provided to SEDC's utilities such as lockbox, credit cards, return check collection, e-checks and MasterCard RPPS-On-Line Payments. SEDC is currently in the final stage completing PCI compliance requirements mandated by the credit card theft regulatory arm known as the PCI Council. Meeting the PCI compliance requirements ensures that extreme measures and policies have been adopted to detect, prevent, and mitigate the risk of credit card information being stolen or improperly accessed, which is a subset of identity theft (See example Acknowledgement and Receipt of Payment Card Industry [PCI] Data Security Standards [DSS] Awareness form – Page 7).

Additionally, many of these policies and procedures from the PCI compliance project have been applied to the other financial service products.

SEDC

Southeastern Data Cooperative

GIVEN TO SEDC AND SUBSIDIARY EMPLOYEES

Acknowledgment and Receipt of Identity Theft Policy

Identity theft is fraud committed or attempted by using the identifying information of another person without his or her authority. Identifying information may include such things as their name, address, Social Security number, account number, date of birth, driver's license number, and other unique electronic identification numbers or codes. SEDC provides software to utilities that stores a great deal of this type of information in an electronic format.

Based on the FTC's Fair & Accurate Credit Transactions Act of 2003, financial institutions, creditors and ***utilities*** are required to establish an "Identity Theft Prevention Program". The primary objectives of this program are to detect, prevent and mitigate identity theft. While SEDC is not a financial institution, creditor or utility, SEDC's employees have access to utilities' consumer and employee personal information.

Therefore, SEDC has adopted an "Identity Theft Prevention Program."

While many elements of the Identity Theft Prevention Program documentation already exist in SEDC's Electronics Communication Policy, Information Security Policy, PCI Security Standards document and Acknowledgment and Receipt of Payment Card Industry (PCI) Data Security Standards (DSS) Awareness document, this document - the ***Acknowledgement and Receipt of Identity Theft Policy,*** is designed to bring full attention to acceptable work procedures relating to SEDC's customer data.

The following are key points to the Identity Theft Prevention Program:

- Access into customer's systems, which includes a customer's database residing in the SEDC facility, is strictly prohibited unless permission has been given by the customer to access those systems and or database(s).

- Personal information from a customer's system is not to be downloaded, copied, or otherwise retrieved, if at all possible.

- The customer will be notified of the information retrieved, if it does become necessary to download, copy, or retrieve personal information stored on a customer's system.

- Under NO CIRCUMSTANCE will personal information stored on a customer's system be distributed to any third party without the written consent of the customer's management.

- Personal information that is appropriately retrieved from a customer's system will be placed in a secure location at the end of each working day.

- Personal information that is appropriately retrieved from a customer's system and printed will be shredded once its useful life has expired.

- The duty of all managers, supervisors, and employees is to ensure that the above points are adhered to and monitored through observations and proprietary reporting systems. Violations from the above points are to be escalated to any and all senior management including the CEO.

Your signature below indicates that you have read the above and have full understanding of the above. Failure to comply with the above policy ***WILL LEAD*** to disciplinary action. This disciplinary action may include termination.

Printed Name of Employee: ______________________________

Employee's Signature: __________________________________ Date: _______

Printed Name of Management Witness: ____________________

Manager's Signature: ___________________________________ Date: _______

GIVEN TO SEDC AND SUBSIDIARY EMPLOYEES

Acknowledgment and Receipt of Payment Card Industry (PCI) Data Security Standards (DSS) Awareness

Since part of SEDC's business includes a Financial Services department that processes credit card transactions, all employees of the Company are expected to understand the importance of preserving the security of any and all credit card information. PCI defines **PAN** (Primary Account Number) as the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. It is generally just called the credit card account number.

For organizations that process credit card payments, PCI requires that policies, procedures and practices are in place that ***precludes*** the sending of unencrypted PANs by e-mail.

It is therefore the policy of SEDC that e-mailing unencrypted PAN is strictly prohibited by all employees of SEDC. There may be times when e-mailing encrypted PAN will be a necessity and in those cases the IT department must be contacted and Financial Services management must provide pre-approval in writing or by email.

Your signature below indicates that you have read the above and have full understanding of the above. Failure to comply with the above policy may lead to disciplinary action, up to and including termination.

Printed Name of Employee: ______________________________

Employee's Signature: __________________________________ Date: _______

Printed Name of Management Witness: ____________________

Manager's Signature: ___________________________________ Date: _______

BIG SANDY RURAL ELECTRIC COOPERATIVE CORPORATIVE
POLICY NO. 300-099
SECTION C

SUBJECT: **Big Sandy RECC** has developed an **Identity Theft Prevention Program.**

OBJECTIVE: Designed to detect, prevent and mitigate theft in connection with the opening or maintaining of any covered account. The program is consistent with the utility's mission to provide safe and reliable electricity at the lowest possible price, while being an active and supportive part of the communities we serve.

Privacy Committee

On November 1, 2008, the Privacy Committee was formed under the leadership of representation from key areas included:

Name	Department	Responsibilities
Jeff Prater	Senior Management	**Operations Management Field Employees**
Sandra Shepherd	Accounting	**Billing & Collections Expert in the Flow of Funds**
Adam Ferguson	IT	**Data and Network Security Expert in Network Admin.**
Trish Baldwin	Payroll & HR	**Employee-Employer related business. Personnel Information. Identify Theft Training**
Angie Stewart	Customer Resources	**Day to day processes in opening new accounts and monitoring activity of existing accounts**

Judy McClure	HR & Administration	**Privacy Officer** **Will coordinate activities of the committee, develop and evaluate program** **Reports to Senior Mgt & Board of Directors**

Our Privacy Committee will attend scheduled meetings every six months, and minutes will be taken. An annual report will be presented to the Board for review. A Policy handbook (manual) will be used in establishing guidelines and regulations and will be administered to train all necessary employees.

I. Purpose:

The goal of this policy is to prevent identity theft. Big Sandy RECC recognizes the responsibility to safeguard personal customer information within the workplace. The purpose of this policy is to create an Identity Theft Prevention Program utilizing guides set forth in the FACT Act (2003).

II. Scope:

This policy applies to management and all personnel of Big Sandy RECC. The following represents a policy for the development of the Identity Theft Prevention program. Company may already have policies written and developed, which can be incorporated into the program. This does not replace, but rather supplements, any standing policies.

III. Responsibility:

Big Sandy RECC must protect customer data and implement policies and procedures that meet standards established by the Federal Trade Commission by

May 2009

IV. Definitions:

IT – Information Technology

Identity Theft – Financial identity theft occurs when someone uses another consumer's personal information (name, social security number, etc.) with the intent of conducting multiple transactions to commit fraud that results in substantial harm or inconvenience to the victim. This fraudulent activity may include opening deposit accounts with counterfeit checks, establishing credit card accounts, establishing lines of credit, or gaining access to victim's accounts with the intent of depleting the balances.

Company – For the purposes of this policy, Big Sandy RECC is referred to as Company.

Red Flag – A pattern, particular specific activity that indicates the possible risk of identity theft.

V. Procedure:

A. Implementing the Program

1. Form an Identity Theft Prevention Protection Committee. Establish an Identity Theft Prevention Committee to create, drive and monitor the program. Select members from Senior Management, Accounting, IT, Human Resources, Administration and Customer Service.

2. Assign Responsibilities to Committee Members.

3. Appoint a Privacy Officer

   Privacy officer functions as the head of committee. He/she reports to a member of Senior Management, i.e.: General Manager regarding the outcomes and needs of the identity theft prevention program.

B. Assess Company's Need for New/Updated Policies and Procedure

The following represent the core of the procedures for the Identity Theft Prevention Program. Please modify to meet the needs and standards of your utility. Add related policies such as "Use of Passwords," as they are already established.

IV. Providing Designated Employees with Identity Theft Prevention Training

1. Designated employees will be trained on a need to know basis according to job responsibilities.

2. Initial training is provided on 3 levels:

   Committee members participated in a 12 hour professional association Identity Theft Prevention Program workshop covering principles of needs assessment, program design, development, implementation and evaluation. Strategies for revision and reporting were included. Committee members unable to attend will receive one on one training by a workshop attendee.

   Supervisors – Initial two hour program addresses supervisory role in preventing identity theft.

   Employee – Initial two hour program addresses the safeguarding of secured information.

3. Annual Updates will be provided for all designated employees. Sessions to be a minimum of 30 minutes will include, but not limited to:

   · Patterns of incidents, changes in informational technology, changes in methods of Identity theft, results of evaluations, employee's input on strategies for enhancing Identity Theft Prevention Program.

4. Documentation of Training

Needs Assessment

On November 1, 2008, Big Sandy RECC conducted a needs assessment of the flow of secured information during the processes of opening a new account as well as monitoring transactions on existing accounts. A review of red flags in the industry and the examples outlined in the FACT Act legislation served as the basis for comparing present policies and procedures against those needed to detect, prevent and mitigate identity theft. The following strengths and areas for improvement were identified:

Opening Accounts:

Strengths: Photos IDs, such as State ID card, Driver's License and obtaining a social security card. Using Online Utility to verify. Computer monitors hid away from plain view.

Areas for Improvement: Opening accounts in a private office so no one can over hear conversation. Keeping service order out of view and removing social security off of service orders. Shred all notes!

Monitoring Transactions in Existing Accounts:

Strengths: Online bill payments – When someone calls in we ask questions long the lines of social security number, telephone number, address and password questions that they have setup. If someone calls for help on setting an online account up, we verify again with the social security number and address questions. If someone tries to use it to setup a new account, we know they already have an existing account because we monitor social security numbers.

Areas for Improvement: Monitoring credit card use with credit card logs. Locking computer down when CSR leaves for break!! New user log in and out when filling in for the CSRs, so not just anyone can look at the information on the screen by walking around to it. When mail is being dropped off, it is handed to an employee and not just set down on a desk when someone is not at that desk!!!

)a **June 18, 2007**

'o: **All SEDC Customers**

'ubject: **Credit Card Payments**
Payment Card Industry (PCI)
Data Security Standards (DSS)

Vhat is PCI DSS?
n an effort to ensure that consumer credit card information remains secure and protected, the credit card industry ha reated a standard known as PCI DSS, which stands for Payment Card Industry Data Security Standard. This standard i: onsidered to be a *"best practices"* guideline to help organizations process credit card payments, prevent credit card fraud acking and various other security issues.

'he PCI DSS reflects the combined interests of VISA, MasterCard, Discover and American Express and represents aı greed upon set of security standards which Merchants, such as SEDC and Service Providers must become compliant. A lready mentioned; PCI DSS outlines "best practices" for any and all credit card data that is stored, processed, o :ansmitted. The scope of these "best practices" is comprised of 12 requirement areas of common safeguards and dat: rotection measures which must be put in place in order to ensure confidentiality, integrity, privacy, and accountability fo ardholder data.

VI s SEDC going to do?
:urrently SEDC is proactively moving towards PCI compliance and the purpose of this memo is to give you aı nderstanding of how your organization will be affected.

)ue to the extensive scope which PCI covers, independent professionally certified PCI consultants hired by SEDC havı dvised that the most practical approach is to first remove SEDC's customers from the scope covered by PCI. This i: ccomplished by gradually realigning the credit card payment application such *that no credit card information is stored iı ny place at any customer location. This means all credit card information currently stored in databases, log files, PC 'isk drives, backup tapes and any printed information, must be 100% eliminated.*

Vhile this may seem extreme, it is the only approach that completely removes our 200+ utility customer's physical locatioı rom the scope of the PCI radar. Any approach short of this leaves customers under the scope of PCI compliance and baseı n the 12 requirements mandated by PCI, the task of SEDC, (as the sole merchant for all of SEDC's customers), becomin; 'CI compliant is not only impractical, it is quite likely, not possible.

'his in no way means there will be a disruption in payments made by credit cards; only that payment information will nı ɔnger be stored at the customer's physical location.

t is our intent that SEDC's execution of this change will go largely unnoticed by SEDC's customers as well as SEDC': ustomer's customer.

How will SEDC's customers be affected?
The timeline set for compliance has been set to occur within the next 12 months. Below is a brief list of what customer can expect to occur:

1. Credit Card Payment applications will be changed so that no CVV2 codes are stored in the customer's database and existing CVV2 codes will be deleted from the database. However, CVV2 code data that is keyed wi continue to transmit in processing a credit card payment.

2. Credit Card Payment applications will be changed so that no credit card numbers are stored in the customer' database or log files and existing credit card numbers will be deleted from the database. Also at this stage, CVV2 code will no longer be written to log files.

3. All allowable credit card data that can be stored for all of SEDC's customers will be stored in a PCI complian encrypted format at SEDC within PCI compliant network infrastructures.

4. Any external device, e.g. an IVR system, which transmits credit card payment data into a customer's physica location(s), cannot *store* credit card data on any media either inside or outside the physical location of the custome If such a system does exist, the utility must adopt a solution that does not *store* credit card information in any plac or discontinue use of such a system. If this is not accomplished to SEDC's satisfaction, SEDC will be forced to tur off all credit card processing payment methods for that customer until such time as the problem is remedied t SEDC's satisfaction. Again, this is the *only way* to remove SEDC's customers from the scope of PCI.

5. While it is true that SEDC's credit card application and policies will remove customers from the scope of PC customers may choose to explore credit card application systems that are different than those of SEDC. Therefore SEDC will seek indemnification in which a customer holds SEDC harmless in the event the customer takes action independent of SEDC's credit card application and PCI policies which put the customer back in the scope of PCI.

Additionally, customers will need to sign-off that no credit card information remains stored at their location i *any manner* including: databases, log files, PC disk drives, tapes, printed material, etc.

SEDC has made this a top priority and is committed to ensuring consumer credit card information remains secure an protected by adhering to the standards of PCI.

We appreciate your current support of SEDC and your future support in this endeavor.

Sincerely,

Ron Camp
CEO
Southeastern Data Cooperative, Inc.

BIG SANDY RURAL ELECTRIC COOPERATIVE CORPORATION

POLICY STATEMENT NO. 300-180

SECTION C

SUBJECT: Records Management Policy.

Purpose: The purpose of this policy is to ensure the reasonable and good faith retention of all records created by or under the control of the Cooperative, whether paper or electronic, that are necessary or advisable to retain for: business operations; historical value; accounting, audit, tax and financial purposes; compliance with applicable law; possible future use in litigation involving the Cooperative; and possible future use in an official proceeding or governmental investigation, audit or other matter. Other records, which are not necessary to retain for these reasons, shall be destroyed in accordance with the guidelines set forth in this policy. All other information that is not a record should be discarded after it has fulfilled its purpose to avoid the unnecessary expenses and effort that would be required to preserve it. A legal hold notice shall be issued when it becomes necessary to preserve a record or other information otherwise scheduled or due for ordinary and appropriate destruction in accordance with this policy.

Policy: Records of the Cooperative, which may be in electronic or paper form, shall be retained in accordance with these guidelines. Records that do not need to retained shall be destroyed after the requisite retention period, if any, has passed. A log or other documentation of records destruction may be created to track compliance and assist in evaluating the effectiveness of this policy. Pending or potential litigation, governmental investigation and other circumstances may require a "hold" or suspension of regularly scheduled destruction of records or other information. Employees will be promptly notified of any such hold by President/General Manager. The format of the hold notification is shown in appendix III to this policy.

Definitions: Unless otherwise indicated in this policy, the following terms will have the meanings provided in this section.

Active Data/Records - electronic or paper records and information that are presently in use or are immediately accessible to users.

Archival Data/Records - electronic or paper records and information that are not directly accessible to users, but which are maintained long term and accessible with some effort.

Backup Data/Records - electronic or paper records and information that are not presently in use and which are routinely stored on portable media (e.g. disk, magnetic tape) and/or off-site and are a source for disaster recovery.

Distributed Data/Records-data living on portable media or "non-local" devices (e.g. PDAs, BlackBerrys, employee home computer, application service provider, ISPs). Most is probably "active" data.

ESI- "Electronically Stored Information" - any file, document, data, image, database,etc. that is stored on a computing device or electronic media, including but not limited to serves, computer desktops and laptops, cell phones, hard drives, flash drives, PDAs or BlackBerrys, CDs or DVDs, floppy disks, and magnetic tapes.

Legacy Data- information which has retained some importance or usefulness to the Cooperative for a period of time but has been created or stored by the use of software and/or hardware that has subsequently become obsolete or been replaced ("legacy systems").

Record - A "record" is any information (paper or electronic) recorded in a tangible form that is created or received by the Cooperative and documents some aspect of its operations. A record has some enduring value to the Cooperative that merits its retention for some period of time. Records include original and copies of contracts and other legal documents, memos, reports, forms, checks, accounting journals and ledgers, work orders, drawings, maps, images, photographs, and may be found in various electronic or machine-readable formats, including without limitation, CD-ROMs, DVDs, tape recordings, voice mail messages, e-mails, microfiche, web pages, computer and other electronic files.

Other information/Data-"Other information" or "data" is any other material that is of a transitory nature, that after serving its limited purpose or being transferred to a more permanent form, or being incorporated with other record materials, Cooperative has no need to retain such information except in the event of a legal hold. Some examples are: notes, drafts, routine correspondence, informational or courtesy copies, extra copies of filed or preserved records, and emails containing non-record information (such as scheduling or logistics information, thank you notes, etc;).

Retention of Records: Records shall be indexed and retained in a manner that ensures their easy accessibility. Records shall be maintained for as long as the period stated in the schedule appended to this policy, which schedule is based on the minimum periods required by applicable state or federal law and necessity for ongoing business purposes. The retention schedule will be reviewed periodically and amended as needed to reflect changing legal requirements, business needs or evolving practices. Designated individuals(s) shall be deemed the Records Custodian responsible for supervising all of the Cooperative's retention practices and procedures and ensuring that appropriate internal controls are implemented. Paper and electronic records and other information shall be maintained in the formats and/or media and at the locations provided in the master index, which media shall ensure a life expectancy that, at a minimum, preserves the records for as long as specified in the schedule. All records that require transfer to storage media that is different from the media in which the document was originally created or is being maintained requires documentation of the transfer and verification for accuracy.

Destruction of Records & Other Information: Unless a legal hold is in effect, destruction of records shall occur within 6 months after the time period stated in the schedule has been met. Other information should be discarded as soon practicable after it has served its purpose unless subject to a legal hold.

Destruction may occur by the following acceptable methods:
(Paper)

- Recycling or trash if no sensitive, personally identifiable or confidential information is included
- Shredding, burning, or pulverizing if sensitive, personally identifiable or confidential information is included

(Electronic)

- Deletion of records and data on shared network files, computer desktop and laptop hard drives, including personal copies
- Deletion of distributed data/records on peripheral devices and portable storage media (e.g. PDAs, memory sticks, CDs, floppy disks, etc.)
- Erasing or recycling of magnetic tapes

Suspension of Destruction/ "Legal Hold": A legal hold is the process for suspending the destruction of records and other information that becomes necessary for the Cooperative to preserve. A legal hold may need to be issued for various reasons, such as:

- A complaint is filed against the Cooperative
- A credible threat of litigation has been received by the Cooperative
- A discovery request is received
- A records preservation order has been issued
- A subpoena has been served on the Cooperative
- A governmental, regulatory or law enforcement agency has instituted an investigation
- An event has occurred that resulted in death or serious bodily injury
- A circumstance has arisen that is likely to cause the Cooperative to file a lawsuit against someone or some entity
- An employee has made a complaint/allegation/report regarding a violation of law, Cooperative policy, or other improper conduct prompting an internal investigation

If a staff member of Cooperative receives any such complaint, request, subpoena or inquiry, he or she should immediately submit it to the direct supervisor. Following consultation with legal counsel, a determination will be made regarding the need to preserve records. If such a need is determined to exist, then the Cooperative's attorney will issue a legal hold notification in the form appended to this policy (Appendix III).

The legal hold requires the preservation of all records and other information detailed in the legal hold notice. With regard to electronic records and information, all such active, distributed and archived materials must be preserved. Back-up tapes that only contain records or other information redundant to that which is being maintained as active or archived data, will be recycled or destroyed in accordance with the Cooperative's regular back-up tape policy/practice.

If a computer or peripheral device (e.g. BlackBerry, external disk drive, etc.) has stored on it records or other information subject to the legal hold, then any schedule replacement of that computer or device must be suspended until the stored materials on such computer or device are copied to a secure medium before the computer or device is taken out of service. Such steps must be documented (in a hardware replacement, IT maintenance, or other log) noting the dates of such copying and the equipment replacement, the person responsible for the copying and replacement, and the location of the copied materials.

Compliance & Questions: Every employee, director and agent of the Cooperative is required to comply with this policy. Training will be provided as needed to ensure that everyone subject to the policy is familiar with its provisions and understands the specific responsibilities and tasks associated with carrying out the policy. Every person subject to the policy shall sign a copy of the acknowledgement appended to this policy. Periodic compliance audits and testing of retention, legal hold, and destruction procedures will be undertaken at the direction and supervision of the Records Custodian. The President/General Manager shall make periodic reports to the Board of Directors regarding overall compliance.

Questions about this policy should be directed to: The Records Custodian

Reporting of Suspected Noncompliance: Should any employee, director or agent to the Cooperative become aware of information indicating that a person responsible for the retention or destruction of records is not in compliance with this policy, such information shall be promptly reported to the Records Custodian.

Effective Date: This policy is effective as of 3-18, 2009. A review of this policy will take place at least periodically at which time amendments to the policy may be made as necessary. This policy has not been amended.

3-18-09
Adopted (date)

Secretary-BSRECC

Appendix II

Retention Schedule

(Note: Rural Utilities Service borrowers should refer to Subpart D of 7 C.F.R. § 1767 and FERC's regulations at 18 C.F.R. § 125. As noted in the sample policy, RUS issued records preservation rules in May 2008 that codify the FERC requirements and RUS Bulletin 180.2. The retention periods specified here are largely based on FERC's retention schedule for basic books of account found at 18 C.F.R. § 125.3, with deviations and suggested additions noted in Arial font and italicized. RUS regulations note that RUS reserves "the right to add records, or lengthen retention periods upon finding that retention periods may be insufficient for its purposes." 7 C.F.R. § 1767.69(a). Also, please note that the RUS regulatory text states that: "Records of [] a kind not listed in the FERC regulations should be governed by those applicable to the closest similar records." § 1767.71(a).)

Record Description ***(Include any identification numbers, etc.)***	**Retention Period**
Corporate & General: 1. Reports to stockholders: Annual reports or statements to stockholders.	5 years *[State enabling statutes that track the Model Business Corporation Act or Model Nonprofit Corporation Act would likely have a requirement to maintain copies of all communications to shareholders or members for 3 years.]*
2. Organizational documents: (a) Minute books of member, board and board committee meetings; *Record of all actions taken by the shareholders or board without a meeting; all actions taken by a committee of the board in place of the board on behalf of the corporation* (b) Titles, franchises, and licenses: Copies of formal orders of regulatory commissions served upon the utility, if applicable. *(c) Articles and amendments in effect; Bylaws and amendments in effect; Board resolutions regarding member classes or rights*	(a) Permanently *[Many states require minutes to be preserved permanently. FERC: 5 years or termination of the corporation's existence, whichever occurs first.]* (b) 6 years after final non-appealable order *(c) Indefinitely*
3. Contracts, including amendments and agreements (except contracts provided for elsewhere): (a) Service contracts, such as for management, accounting, and financial services. (All contracts, related memoranda, and revisions.) (b) Contracts with others for transmission or the purchase, sale or interchange of product. (All contracts, related memoranda, and revisions) (c) Memoranda essential to clarifying or explaining provisions of contracts listed above, including requests for discounts. (d) Card or book records of contracts, leases, and agreements made, showing dates of expirations and of renewals, memoranda of receipts, and payments under such contracts.	(a) 4 years after expiration or until the conclusion of any contract disputes pertaining to such contracts, whichever is later (b) 4 years after expiration or until the conclusion of any contract disputes or governmental proceedings pertaining to such contracts, whichever is later *[Cooperatives should consider keeping FEMA mutual aid agreements indefinitely, though NRECA maintains a centralized database of all such agreements that it receives.]* (c) & (d) For the same periods as contracts to which they relate

© NRECA 2008.

4. Accountants' and auditors' reports: (a) Reports of examinations and audits by accountants and auditors not in the regular employ of the utility. (b) Internal audit reports and working papers	(a) & (b) 5 years after the date of the report
Information Technology Management: 5. Automatic data processing records (retain original source data used as input for data processing and data processing report printouts for the applicable periods prescribed elsewhere in the schedule): Software program documentation and revisions thereto.	Retain as long as it represents an active viable program or for periods prescribed for related output data, whichever is shorter.
General Accounting Records: 6. General and subsidiary ledgers: (a) Ledgers: (1) General ledgers (2) Ledgers subsidiary or auxiliary to general ledgers except ledgers provided for elsewhere. (b) Indexes: (1) Indexes to general ledgers (2) Indexes to subsidiary ledgers except ledgers provided for elsewhere. (c) Trial balance sheets of general and subsidiary ledgers	(a)(1) & (2) 10 years (b)(1) & (2) 10 years (c) 2 years
7. Journals: General and subsidiary	10 years
8. Journal vouchers and journal entries including supporting detail: (a) Journal vouchers and journal entries (b) Analyses, summarization, distributions, and other computations which support journal vouchers and journal entries: (1) Charging plant accounts (2) Charging all other accounts	(a) 10 years (b)(1) 25 years. See § 125.2(g). (b)(2) 6 years
9. Cash books: General and subsidiary or auxiliary books	5 years after close of fiscal year.
10. Voucher registers: Voucher registers or similar records when used as a source document.	5 years. See § 125.2(g)
11. Vouchers: (a) Paid and canceled vouchers (one copy-analysis sheets showing detailed distribution of charges on individual vouchers and other supporting papers). (b) Original bills and invoices for materials, services, etc., paid by vouchers. (c) Paid checks and receipts for payments of specific vouchers. (d) Authorization for the payment of specific vouchers (e) Lists of unaudited bills (accounts payable), list of vouchers transmitted, and memoranda regarding changes in audited bills. (f) Voucher indexes	(a) , (b) & (d) 5 years. See § 125.2(g). *[Cooperatives may wish to hold these records for a longer period as historical evidence of the "reasonable cost" for work and services performed in response to a disaster that is the subject of FEMA reimbursement. FEMA regulations require records related to claims to be kept for 3 years, unless any litigation, claim, negotiation or other audit is ongoing. See 44 C.F.R. § 13.42(b) and FEMA Publication 322, "Public Assistance Guide" available at www.fema.gov/government/grant/pa/pag07_t.shtm.]* (c) 5 years. (e) Destroy at option (f) Destroy at option

11a. Financial requirement and expenditure statements, which are not otherwise reflected in this schedule	*1 year after the "as of date" of RUS' loan fund and accounting review [RUS rule. Typically, RUS field accountants audit a borrower every 2 or 3 years, in tandem with a review of financed construction. So, 1 year after the audit is completed and accepted.]*
Insurance: 12. Insurance records: (a) Records of insurance policies in force, showing coverage, premiums paid, and expiration dates. (b) Records of amounts recovered from insurance companies in connection with losses and of claims against insurance companies, including reports of losses, and supporting papers. *(c) Applications for insurance policies in force.*	(a) Destroy at option after expiration of such policies *[Before destroying any policy, cooperatives should determine whether the policy is a "claims made" or "occurrence" policy. Under the latter, the policy that is in force on the date of the event that caused the loss is the policy that will cover that loss. Because claims can arise years after a policy has expired, expiration may not always be the appropriate time to destroy.]* (b) 6 years. See § 125.2(g). *(c) Destroy at option after expiration of such policies' coverage period. [This is an additional recommendation and not required by FERC regulations or RUS' proposed rule as insurers could seek to cancel or void a policy to avoid liability on the grounds that an application contained materially false or omitted materially significant information.]*
Operations and Maintenance: *(13.1 & 13.2 Relate to Power Generation Equipment and have not been included.)*	
14. Transmission and distribution: (a) Substation and transmission line logs (b) System operator's daily logs and reports of operation (c) Transformer history records (d) Records of transformer inspections, oil tests, etc. *(e) Records of other inspections, assessments, tests of component parts of the utility system, and Emergency Restoration Plan exercises*	(a) & (b) 3 years (c) Life of transformer (d) Destroy at option *(e) At least until the next applicable inspection, test, etc. is conducted [This is a suggested addition for RUS borrowers pursuant to 7 C.F.R. Part 1730.]*
15. Maintenance work orders and job orders: (a) Authorizations for expenditures for maintenance work to be covered by work orders, including memoranda showing the estimates of costs to be incurred. (b) Work order sheets to which are posted in detail the entries for labor, material, and other charges in connection with maintenance, and other work pertaining to utility operations. (c) Summaries of expenditures on maintenance and job orders and clearances to operating other accounts (exclusive of plant accounts).	(a) – (c) 5 years

© NRECA 2008.

Plant and Depreciation: 16. Plant ledgers: (a) Ledgers of utility plant accounts including land and other detailed ledgers showing the cost of utility plant by classes. (b) Continuing plant inventory ledger, book or card records showing description, location, quantities, cost, etc.,.of physical units (or items) of utility plant owned. *(c) Life & mortality study data for depreciation purposes*	(a) & (b) 25 years. See § 125.2(g). *[Per RUS rule, "...records related to plant in service must be retained until the facilities are permanently removed from utility service, all removal and restoration activities are completed, and all costs are retired from the accounting records unless accounting adjustments resulting from reclassification and original costs studies have been approved by [RUS] or other regulatory body having jurisdiction."]* *(c) 25 years or for 10 years after plant is retired, whichever is longer. [Per RUS rule. This is relevant for those borrowers that do not use RUS' standard depreciation rates.]*
17. Construction work in progress ledgers, work orders, and supplemental records: (a) Construction work in progress ledgers (b) Work orders sheets to which are posted in summary form or in detail the entries for labor, materials, and other charges for utility plant additions and the entries closing the work orders to utility plant in service at completion. (c) Authorizations for expenditures for additions to utility plant, including memoranda showing the detailed estimates of cost, and the bases therefor (including original and revised or subsequent authorizations). (d) Requisitions and registers of authorizations for utility plant expenditures. (e) Completion or performance reports showing comparison between authorized estimates and actual expenditures for utility plant additions. (f) Analysis or cost reports showing quantities of materials used, unit costs, number of man-hours etc., in connection with completed construction project. (g) Records and reports pertaining to progress of construction work, the order in which jobs are to be completed, and similar records which do not form a basis of entries to the accounts.	(a) & (b) 5 years after clearance to plant account, provided continuing plant inventory records are maintained; otherwise 5 years after plant is retired. (c) – (f) 5 years after clearance to plant account except where there are ongoing regulatory commission proceedings (g) Destroy at option
18. Retirement work in progress ledgers, work orders, and supplemental records: (a) Work order sheets to which are posted the entries for removal costs, materials recovered, and credits to utility plant accounts for cost of plant retirement. (b) Authorizations for retirement of utility plant, including memoranda showing the basis for determination to be retired and estimates of salvage and removal costs. (c) Registers of retirement work	(a) & (b) 5 years after plant is retired (c) 5 years

© NRECA 2008.

19. Summary sheets, distribution sheets, reports, statements, and papers directly supporting debits and credits to utility plant accounts not covered by construction or retirement work orders and their supporting records.	5 years *[Per RUS rule, records supporting construction financed by RUS "shall be retained until audited and approved" by RUS.]*
20. Appraisals and valuations: (a) Appraisals and valuations made by the company of its properties or investments or of the properties or investments of any associated companies. (Includes all records essential thereto.). (b) Determinations of amounts by which properties or investments of the company or any of its associated companies will be either written up or written down as a result of: (1) Mergers or acquisitions (2) Asset impairments (3) Other bases	(a) 3 years after appraisal (b)(1) 10 years after completion of transaction or as ordered by regulatory commission, if applicable (b)(2) 10 years after recognition of asset impairment. (b)(3) 10 years after the asset was written up or down
21. The original or reproduction of engineering records, drawings, and other supporting data for proposed or as-constructed utility facilities: Maps, diagrams, profiles, photographs, field survey notes, plot plan, detail drawings, records of engineering studies, and similar records showing the location of proposed or as-constructed facilities.	Retain until retired
22. Contracts relating to utility plant: (a) Contracts relating to acquisition or sale of plant (b) Contracts and other agreements relating to services performed in connection with construction of utility plant (including contracts for the construction of plant by others for the utility and for supervision and engineering relating to construction work).	(a) & (b) 6 years after plant is retired or sold
23. Records pertaining to reclassification of utility plant accounts to conform to prescribed systems of accounts including supporting papers showing the bases for such reclassifications.	6 years
24. Records of accumulated provisions for depreciation and depletion of utility plant and supporting computation of expense: (a) Detailed records or analysis sheets segregating the accumulated depreciation according to functional classification of plant. (b) Records reflecting the service life of property and the percentage of salvage and cost of removal for property retired from each account for depreciable utility plant.	(a) & (b) 25 years

© NRECA 2008.

Purchase and Stores: 25. Procurement: (a) Agreements entered into for the acquisition of goods or the performance of services. Includes all forms of agreements not specifically set forth in Subsection 7 such as but not limited to: Letters of intent, exchange of correspondence, master agreements, term contracts, rental agreements, and the various types of purchase orders: (1) For goods or services relating to plant construction (2) For other goods or services (b) Supporting documents including accepted and unaccepted bids or proposals (summaries of unaccepted bids or proposals may be kept in lieu of originals) evidencing all relevant elements of the procurement.	(a)(1) 6 years. See § 125.2(g). (a)(2) 6 years (b) 6 years. See § 125.2(g).
26. Material ledgers: Ledger sheets of materials and supplies received, issued, and on hand	6 years after the date the records/ledgers were created
27. Materials and supplies received and issued: Records showing the detailed distribution of materials and supplies issued during accounting periods	6 years. See § 125.2(g).
28. Records of sales of scrap and materials and supplies: (a) Authorization for sale of scrap and materials and supplies. (b) Contracts for sale of scrap materials and supplies	(a) & (b) 3 years
Revenue Accounting and Collecting: 29. Customers' service applications and contracts: Contracts, including amendments for extensions of service, for which contributions are made by customers and others	4 years after expiration
30. Rate schedules: General files of *[FERC: published]* rate sheets and schedules of utility service. Including schedules suspended or superseded.	6 years after published rate sheets and schedules are superseded or no longer used to charge for utility service
31. Maximum demand, and demand meter record cards	1 year, except where the basic chart information is transferred to another record the charts need only be retained 6 months, provided the basic data is retained 1 year.

© NRECA 2008.

32. Miscellaneous billing data: Billing department's copies of contracts with customers (other than contracts in general files) *(a) "Consumer accounts' records"*	Destroy at option *(a) "Kept for those years for which patronage capital has not been allocated" [This is language in RUS' new rule. Typically, such allocations are done annually. It probably makes sense, to retain records indicating the last known address for members and patrons with their annual patronage totals for at least as long as the cooperative's capital credit rotation cycle or preferably permanently. Permanent retention is probably needed for a few reasons. One reason is that if the cooperative is making early capital credit retirements at a discount, then the co-op will need to keep such records permanently or until after liquidation of the cooperative. Further, see Rev. Ruling 72-36, which requires the allocation of the appreciated value of real property to patrons. See also, applicable state dissolution statutes that may require allocation at dissolution based on historical patronage.]*
33. Revenue summaries: Summaries of monthly operating revenues according to classes of service. Including summaries of forfeited discounts and penalties	5 years
Tax: 34. Tax records: (a) Copies of tax returns and supporting schedules filed with taxing authorities, supporting working papers, records of appeals of tax bills, and receipts for payment. See Subsection 11(b) for vouchers evidencing disbursements: (1) Income tax returns *(e.g. IRS Form 990s, including amended returns)* (2) Property tax returns (3) Sales and other use taxes . (4) Other taxes (5) Agreements between associate companies as to allocation of consolidated income taxes. (6) Schedule of allocation of consolidated Federal income taxes among associate companies. (b) Filings with taxing authorities to qualify employee benefit plans. (c) Information returns and reports to taxing authorities. *(d) Tax exemption application and determination letter (e.g. currently, Form 1024, and all accompanying documentation) and any IRS rulings (e.g. private letter ruling)*	(a)(1), (2), (4) - (6) 2 years after final tax liability is determined. *[Forms 990 should be retained for at least 3 years after the due date or filing date of the return, whichever is later to meet public inspection requirements. See I.R.C. § 301.6104(d)-1.]* (a)(3) 2 years (b) 5 years after discontinuance of plan. (c) 3 years after final tax liability is determined *(d) Permanently*

Treasury: 35. Statements of funds and deposits (a) Statements of periodic deposits with fund administrators or trustees. (b) Statements of periodic withdrawals from fund (c) Statements prepared by fund administrator or trustees of fund activity including: (1) Beginning of the year balance of fund; (2) Deposits with the fund; (3) Acquisition of investments held by the fund; (4) Disposition of investments held by the fund; (5) Disbursements from the fund, including party to whom disbursement was made; (6) End of year balance of fund.	*[FERC: For nuclear decommissioning funds, retain records for all items listed for 3 years after final decommissioning is completed. If amortization reserve funds related to licensed projects are maintained, retain until the FERC makes a final determination of the disposition of amortization reserves.]* (a) & (b) Retain records for the most recent 3 years (c) Retain records until the fund is dissolved or terminated
36. Records of deposits with banks and others: (a) Statements from depositories showing the details of funds received, disbursed, transferred, and balances on deposit. (b) Check stubs, registers, or other records of checks issued. *36A. Records of financial commitments with lenders* *(a) loan applications, approval letters & loan contracts* *(b) mortgages, other security instruments associated with loans* *(c) release of lien* *(d) notification from lender to borrower of satisfaction of financial commitment*	(a) Destroy at option after completion of audit by independent accountants. (b) 3 years *(a) & (b) Once a loan or mortgage has been fully paid, these documents, along with receipts or other proof of payment, may be destroyed at a borrower's option. However, retained copies of the executed loan contract and mortgage would be helpful evidence of the requirements to which the borrower was subject during the loan period.* *(c) Permanently* *(d) Permanently*
Miscellaneous: 37. [FERC: Reserved]	
38. Statistics: Financial, operating and statistical reports used for internal administrative or operating purposes.	5 years
39. Budgets and other forecasts (prepared for internal administrative or operating purposes) of estimated future income, receipts and expenditures in connection with financing, construction and operations, including acquisitions and disposals of properties or investments.	3 years
40. Records of predecessor companies	Retain consistent with the requirements for the same types of records of the utility
41. Reports to Federal and State regulatory commissions including annual financial, operating and statistical reports. *[Form EIA-861"Annual Electric Power Industry Report", RUS Form 7, etc.]*	5 years

42. Advertising: Copies of advertisements by or for the company on behalf of itself or any associate company in newspapers, magazines, and other publications, including costs and other records relevant thereto (excluding advertising of appliances, employment opportunities, routine notices, and invitations for bids all of which may be destroyed at option).	2 years
Employment Related: *43. Safety* *(a) Motor vehicle inspection, repair & maintenance records* *(b) CDL driver qualification files* *(c) CDL driver drug & alcohol tests & results* *(d) OSHA 300 Log & OSHA 301 incident reports*	*(a) 1 year and for 6 months after the motor vehicle leaves the motor carrier's control [See 49 C.F.R. § 396.3(c)]* *(b) for 3 years after termination of employment [See 49 C.F.R. § 391.51* *(c) 5 years [See 49 C.F.R. § 382.401]* *(d) 5 years [See 29 C.F.R. § 1904.33 & -.37]*
44. Personnel *(a) Payroll records, collective bargaining agreements* *(b) Performance reviews & other documentation about treatment on the job, job applications and resumes, etc.* *(c) Benefits plan information (ERISA)* *(d) I-9 Forms for all employees hired after 11/6/1986* *(e) Payroll & unemployment taxes* *(f) Wage/earnings records (e.g. time cards, wage rate tables, etc.)* *(g) Dates of FMLA leave, notices to or from employees re FMLA, records of any disputes, etc.*	*(a) 3 years [See 29 C.F.R. § 516.5]* *(b) 3 years for records related to age [See 29 C.F.R. § 1627.3], but 1 year for records related to Title VII & ADA: race, ethnicity, national origin & disability [See 29 C.F.R. § 1602.14]* *(c) At least 6 years after the filing date of the documents [See 29 U.S.C. § 1027]* *(d) for 3 years after the date of hire or 1 year after the date employment is terminated, whichever is later [See 8 C.F.R. § 274a.2]* *(e) 4 years [See IRS Publication 15, Employer's Tax Guide]* *(f) 2 years [See 29 C.F.R. § 516.6]* *(g) 3 years [See 29 C.F.R. § 825.500]*
Environmental: *45. Hazardous Waste/Toxic Chemicals (reports, inspection logs, training records, waste shipment manifests or records, sampling and monitoring data)* *(a) Community Right to Know/TRI reports & supporting documentation* *(b) PCB equipment inspection and maintenance history* *(c) PCB spills* *(d) Used Oil: Spill Prevention Protection & Control plans, procedures and record of tests & inspections* *(e) Haz mat incident reports* *(f) Employee exposures to certain substances (e.g. asbestos, benzene, etc.), including medical evaluations* *(g) Hazardous waste records (shipping manifests, filed reports, test results, etc.)* *(h) Records related to underground storage tanks for fuel (tests results, monitoring, calibration, maintenance or repair records, spills)*	*(a) 3 years from submission of the report [See 40 C.F.R. § 372.10]* *(b) 3 years after disposal [See 40 C.F.R. § 761.30]* *(c) 5 years after clean-up [See 40 C.F.R. § 761.125(a)]* *(d) 3 years [See 40 C.F.R. § 112.7(e)]* *(e) 2 years [See 40 C.F.R. § 171.16]* *(f) 30 years [See, e.g., 29 C.F.R.§§ 1910.1001(m), 1910.20,1910.1028(k)]* *(g) 3 years [See 40 C.F.R. § 262.40]* *(h) 1 year or for another reasonable time period determined by State EPA [See 40 C.F.R. §§ 280.34 &.45]*
46. Water *(a) NPDES Permits & related documentation (including storm water prevention plans, reports, certifications, data used for the notice of intent, etc.)* *(b) Section 404 wetlands permits & related documentation (e.g. related to dredge & fill activities during utility line construction)*	*(a) at least 3 years from the date the permit expires or is terminated [See 40 C.F.R. §122.41(j)(2)]* *(b) varies by state [For example, Virginia requires 3 years from permit expiration. 9 Va. Admin. Code 25-220-80.]*

© NRECA 2008.

Miscellaneous Licenses, Permits & Other Requirements: *47. FCC –* *(a) radio frequency spectrum licenses* *(b) private land mobile radio and microwave station records* *(c) correspondence with the FCC*	*(a) permanently, or until cooperative no longer holds an FCC license* *(b) 1 year [See 47 C.F.R. §§ 90.437 – 90.447 for Private Land Mobile Radio & § 101.217 for Microwave]* *(c) permanently, or until cooperative no longer holds an FCC license*
48. NERC Reliability Standards – (can include audit records, system testing, personnel training, etc.)	*[Varies. Most common is 3 years. But some are less and others are longer. Other standards have no specified retention period but should be maintained to demonstrate compliance in the event of an audit or investigation.]*
Service Related: *49.Records kept in relation to service-related events* *(a) Consumer complaints (including correspondence, voice recordings, investigation reports, etc.)* *(b) Outages (investigation reports, operational records, etc.)* *(c) Accidents (investigation reports, photographs, operational records, etc.)*	*(a) – (c) Until the applicable statute of limitations has passed or litigation is finally decided or settled. (Some state regulatory commissions require the utilities under their jurisdiction to keep records of complaints, outages, and accidents. It would seem prudent that even in the absence of such requirements to maintain appropriate records related to these events in the likely event of subsequent investigation and/or litigation.)*

(Note: "See § 125.2(g)" references are found in the FERC regulations, which section states: "(g) Schedule of records and periods of retention. (1) Records related to plant in service must be retained until the facilities are permanently removed from utility service, all removal and restoration activities are completed, and all costs are retired from the accounting records unless accounting adjustments resulting from reclassification and original costs studies have been approved by the regulatory commission having jurisdiction. If the plant is sold, the associated records or copies thereof, must be transferred to the new owners...." Also, § 125.2 (h) addresses those retention periods designated ***"Destroy at option,"*** *which FERC explains "constitutes authorization for destruction of records at managements' discretion if it does not conflict with other legal retention requirements or usefulness of such records in satisfying pending regulatory actions or directives.")*

Appendix III

Sample Legal Hold Notification

To ensure that every employee, director and agent of ____________ *(Name of Cooperative)* will recognize and respond appropriately to a notification that certain records are now potentially relevant and necessary for litigation or a governmental investigation, this appendix provides a sample legal hold notification.

URGENT NOTICE

TO: *Name all persons identified as likely to have relevant records including the designated Records Custodian or Coordinator*
FROM: *CEO/Cooperative Attorney/Litigation Attorney*
DATE:
RE: *Your Obligation to Preserve Records & Other Information*

The event/circumstance described below has triggered an obligation to preserve records and other information. Your assistance is necessary and required for the preservation of Cooperative's records and other information to fulfill Cooperative's legal obligations and/or preserve Cooperative's rights. Failure to fully comply with this directive could result in harm or penalties against Cooperative; therefore, employees could be subject to discipline, up to and including termination of employment, for failure to follow the directives in this notice.

Event or Circumstance Triggering the Need to Preserve Records *(Description of lawsuit, investigation, occurrence, etc. If litigation, describe specific claims involved.)*

Types of Records & Other Information to be Preserved
All paper and electronic records and other information that could be relevant to the above described event or circumstance must be preserved – that is, retained and not deleted – including, without limitation: *(Tailor description as needed to specific trigger event – such as, documents (including drafts & revisions), spreadsheets (including drafts and revisions), emails (sent & received), databases, calendars, presentations, image files, maps, voice messages, data generated based on Internet activity (cookies, cache, history files), computer usage logs, etc.)*

When potentially relevant records or other information exist on multiple platforms or media, for example: a file on a desktop computer, on a laptop computer, on a mobile device, on a portable storage medium such as a CD-ROM, and a paper copy, every copy must be preserved.

Any routine or planned destruction of these types of records or data that you are aware of and can control (*e.g.* a user's personal email setting to automatically delete messages older than a certain date) must be suspended for the period of this hold.

© NRECA 2008.

Time Period

All of the above described records and other information currently in your possession or under your control must be preserved *(from this point forward until you are notified that this hold is lifted, or state specific time period if known).*

Verification of Preservation

(Describe the actual steps that a recipient of this notice must take to verify preservation. Different types of records or information may require different preservation methods, e.g. certain electronic files may be subject to automatic purging that requires an override or programming change.)

Contact Person(s)

If you have questions regarding this notice, or are aware of any other persons not listed as recipients of this notice –including retired employees, contractors, consultants or others– who should receive this notice, please direct all such questions and information to __________ *(Provide name and contact details of the person overseeing the matter triggering the legal hold, such as the Cooperative's attorney or litigation counsel).*

Reminders

Reminders will be sent to you periodically during the course of this *(litigation, investigation, audit, matter)* to ensure that you continue to preserve relevant information and to inform you of any change as the matter progresses that would affect your preservation obligations. Such a change could include a change in scope that could add additional categories of records or other information for preservation or may require you to take additional preservation or verification steps.

(Note: For helpful guidelines on designing legal hold practices and procedures, see, The Sedona Conference Commentary on Legal Holds: The Trigger & The Process (Aug. 2007 public comment version), available at: http://www.thesedonaconference.org/content/miscFiles/Legal_holds.pdf.

Regarding form & content of the legal hold notification: See also, the Sedona Principles at Comment 5.d: "While the form and content of the notice may vary widely depending upon the circumstances, the notice need not provide a detailed list of all information to retain. Instead, it should describe the types of information that must be preserved, with enough detail to allow the recipient to implement the hold. The notice should state that electronically stored information, as well as paper, is subject to the need for preservation. Additionally, the notice should: (i) describe the subject matter of the litigation and the subject matter, dates, and other criteria defining the information to be preserved; (ii) include a statement that relevant electronically stored information and paper documents must be preserved; (iii) identify likely locations of relevant information (e.g., network, workstation, laptop or other devices); (iv) provide steps that can be followed for preserving the information as may be appropriate; and (v) convey the significance of the obligation to the recipients. The notice need not demand preservation of all documents, only those affected by the preservation obligation Additionally, the preservation obligation, except in extreme circumstances, should not require the complete suspension of normal document management policies, including the routine destruction and deletion of records. Communications should be accomplished in a manner reasonably designed to provide prominent notice to the recipients."

Regarding time period for the hold: In litigation, the hold should remain in effect until the litigation has been finally resolved, either settled or a final judgment issued and the time for all appeals has run. Similarly, in a governmental investigation or audit, the hold should remain in effect until the investigation has been finally concluded, but only if the conclusion of the investigation forecloses the possibility of future prosecution or enforcement actions, check-up audits or inspections, etc.)

Appendix IV

Sample Records Retention Master Index

(Note: As mentioned in the commentary in the sample policy, RUS' record retention requirements include the maintenance of a "master index" of records that identifies the records retained, the retention period, and the location of the records, which shall be subject to RUS review. No specific from or format is specified for the master index – it could be a spreadsheet, a database, a paper list, or a table in a Word document as shown here, for example. The RUS rule also requires that at each office where records are kept or stored, borrowers are to "arrange, file, and index the records currently at that site so that they may be readily identified and made available" to RUS representatives. RUS further requires that documentation be made of transfers to storage media, including verification of accuracy following the transfer, mirroring a FERC regulation. Another requirement is for a certified statement to be appended to the master index regarding any untimely destruction of records, a rough sample of which is provided on the next page. The creation of a "data map" to identify and locate records is typically recommended as an initial step to be completed prior to developing a records management policy. This map could take the form of the master index or vice versa so long as its organization ensures that records are "easily accessible" per RUS' requirement.)

Record Category/Type *(Match with Records Schedule to the extent possible, if desired.)*	**Retention Period**	**Storage Media** *(If stored in a different media from that in which the record was created or being maintained, note the date of the transfer and the date that verification of accuracy was tested.)*	**Location(s)** *(e.g. headquarters file room, off-site storage, network server, vendor's network storage, etc.)*	**Designated Responsible Person/Records Custodian/Records Coordinator**

© NRECA 2008.

Certification of Untimely Destruction or Loss of Records

________________ *certifies that the below identified records were lost/destroyed prior to the expiration of the applicable retention period.*

________________________ ________________

Signature *Date*

________________________ ________________________

Name *Title*

Records Lost or Destroyed Prior to the Expiration of the Retention Period:

Record Description	**Applicable Retention Period**	**Loss or Destruction** *(Describe event or circumstances)*	**Date & Time Loss or Destruction Occurred** *(If not known, it seems to make sense to note when the loss or destruction was discovered.)*

(<u>Note</u>: The RUS rule does not identify any specific format for this certification. This sample contemplates that each destruction or loss event would be noted on a separate statement. Another possible format would be to include a signature and date column in the table of the master index to essentially maintain a running log of untimely destructions or losses.)

Appendix I

Acknowledgment

I acknowledge that I have received and read and that I will abide by this Records Management Policy distributed to me on __________ *(date)*. I understand that I am expected to and agree to bring any questions regarding this policy to the identified contact person(s). I further understand and agree that I am required to complete periodic training on records procedures as a part of this policy.

____
(Signature)

____
(Print Name)

Date: ___________________________

© NRECA 2008.