UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION I
2100 RENAISSANCE BOULEVARD, SUITE 100
KING OF PRUSSIA, PENNSYLVANIA 19406-2713

July 12, 2013

Mr. David A. Heacock
President and Chief Nuclear Officer
Dominion Resources
5000 Dominion Boulevard
Glen Allen, VA 23060-6711

SUBJECT: MILLSTONE POWER STATION - NOTIFICATION OF INSPECTION OF IMPLEMENTATION OF INTERIM CYBER SECURITY MILESTONES 1 - 7

Dear Mr. Heacock:

The purpose of this letter is to notify you that the U.S. Nuclear Regulatory Commission (NRC) staff will conduct an inspection of the implementation of interim cyber security milestones 1 through 7 at Millstone Power Station in November 2013. The inspection team will be led by Mr. John Richmond from the NRC Region 1 Office. The team will be composed of personnel from the NRC Region 1 Office. The inspection will be conducted in accordance with Temporary Instruction 2201/004, "Inspection of Implementation of Interim Cyber Security Milestones 1 - 7."

The schedule for the inspection is as follows:

- Information Gathering Visit: Week of October 21, 2013
- On-site Inspection: Week of November 4, 2013

The purposes of the information gathering visit are to obtain information and documentation needed to support the inspection, to become familiar with the station cyber security program and plant layout, and to obtain plant specific site access training and badging for unescorted site access.

An initial list of the documents the team will review during the conduct of the inspection are listed in the Enclosure. The team leader will contact you with any additional specific document requests prior to the information gathering visit.

Your cooperation and support during this inspection will be appreciated. If you have questions concerning this inspection, or the inspection team's information request or logistical needs, please contact Mr. John Richmond, Team Leader at (610) 337-5220, or via e-mail at john.richmond@nrc.gov.

This letter does not contain new or amended information collection requirements subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). Existing information collection requirements were approved by the Office of Management and Budget, under control number 3150 0011. The NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid Office of Management and Budget control number.

In accordance with 10 CFR 2.390 of the NRC Rules and Practices, a copy of this letter and its enclosures will be available electronically for public inspection in the NRC Public Document Room or from the Publically Available Records (PARS) component of NRC's document system (ADAMS). ADAMS is accessible from the NRC Web site at http://www.nrc.gov/reading-rm/adams.hmtl (the Public Electronic Reading Room).

Sincerely,

/RA/

John F. Rogge, Chief
Engineering Branch 3
Division of Reactor Safety

Docket Nos. 50-336, 50-423
License Nos. DPR-65, NPF-49

Enclosure: Cyber Security Program Supporting Documentation

cc w/encl: Distribution via ListServ

In accordance with 10 CFR 2.390 of the NRC Rules and Practices, a copy of this letter and its enclosures will be available electronically for public inspection in the NRC Public Document Room or from the Publically Available Records (PARS) component of NRC's document system (ADAMS). ADAMS is accessible from the NRC Web site at http://www.nrc.gov/reading-rm/adams.hmtl (the Public Electronic Reading Room).

Sincerely,

/RA/

John F. Rogge, Chief
Engineering Branch 3
Division of Reactor Safety

Docket Nos. 50-336, 50-423
License Nos. DPR-65, NPF-49

Enclosure: Cyber Security Program Supporting Documentation

cc w/encl: Distribution via ListServ

Distribution w/encl: (via E-mail)

W. Dean, RA	**(R1ORAMAIL RESOURCE)**	E. Keighley, DRP
D. Lew, DRA	**(R1ORAMAIL RESOURCE)**	J. DeBoer, DRP
D. Roberts, DRP	**(R1DRPMAIL RESOURCE)**	J. Ambrosini, DRP, SRI
A. Burritt, DRP	**(R1DRPMAIL RESOURCE)**	B. Haagensen, DRP, RI
C. Miller, DRS	(**R1DRSMAIL RESOURCE)**	J. Krafty, DRP, RI
J. Rogge, DRS	**(R1DRSMAIL RESOURCE)**	C. Kowalyshyn, DRP, AA
F. Bower, DRP		V. Campbell, RI OEDO
S. Shaffer, DRP		RidsNrrPMMillstone Resource
J. Richmond, DRS		RidsNrrDorlLpl1-1 Resource

DOCUMENT NAME: G:\DRS\Engineering Branch 3\Richmond\Millstone\MS Cyber 90-Day Letter.doc
ADAMS ACCESSION NUMBER: ML13198A445

☑ SUNSI Review		☑ Non-Sensitive ☐ Sensitive		☑ Publicly Available ☐ Non-Publicly Available	
OFFICE	RI/DRS	RI/DRS			
NAME	JRichmond/	JRogge/			
DATE	07/12 /2013	07/12/2013			

OFFICIAL RECORD COPY

CYBER SECURITY PROGRAM SUPPORTING DOCUMENTATION

If you have any questions regarding this information request, please contact Mr. John Richmond as soon as possible, at (610) 337-5220 or via e-mail at john.richmond@nrc.gov.

Electronic format on compact disc (CD) is the preferred media. If electronic media is made available via an internet based remote document management system, then the remote document access must allow inspectors to download, save, and print the documents in the NRC's regional office. Paper records (hard copy) are of course always acceptable. At the end of the inspection, the documents in the team's possession will not be retained.

Where information is provided that includes tables and/or lists of data or other such information, please do not scan such tables or lists as "images." The preferred file format is a searchable "pdf" file. If possible, CDs should be indexed and hyper-linked to facilitate ease of use.

Safeguards Information should be made available for inspectors use while on-site, and not placed on a data CD. It is not the intent for safeguards information to be transmitted or sent to the Regional office, or retained by an inspector and hand carried off-site. Any exceptions to this will be discussed with appropriate plant staff, on an as-needed basis.

I. Information Requested Prior to the Information Gathering Visit

- The documents requested in this group should be made available to the inspection team in the Region 1 Office, preferably no later than two weeks prior to the Information Gathering Visit.
- This document group is intended to include (1) program and process level information, and (2) milestone specific Non-Safeguards Information.
- Please provide the requested information on three sets of CDs (searchable and hyper-linked, if possible).
- This group of documents should not contain any Safeguards Information.

A. Cyber Security Licensing and Design Basis Documents

1. COPY of all Cyber Security licensing basis documents, including:
   a. Approved Cyber Security Plan (CSP).
   b. Approved CSP Implementation Schedule (e.g., the milestones).
   c. NRC Safety Evaluation Reports for facility CSP.
2. Facility Operating License.
3. Technical Specifications (electronic format only).
4. Technical Requirements Manual or equivalent (electronic format only).
5. Updated Final Safety Analysis Report (electronic format only).

B. Cyber Security Program Supporting Documents

1. COPY of all Cyber Security design basis documents, including industry standards such as Nuclear Energy Institute (NEI) documents.

2 LIST of any "cyber security specific" evaluations, assessments, or calculations.

3. LIST of any single line, elementary, overview, or functional or logic drawings or diagrams issued specifically for cyber security.

4. LIST of any facility drawings or diagrams that were revised or updated in order to implement cyber security (e.g., pre-existing plant drawings that were revised for cyber security).

5. COPY of self assessments, peer assessments, audits, and reviews of the cyber security program for the last two years, including any third party reviews.

6. LIST of Cyber Security related Condition Reports, open or closed within the last two years.

7. LIST of currently scheduled or planned cyber security related modifications to be installed in the plant.

8. COPY of the current cyber security "Health Report," if available.

C. General Facility Information and Documents

1. COPY of the current plant drawings used for operator training that provide additional information on system operation, system operating parameters, setpoints, etc. (e.g., some licensee's refer to these drawings as "Horse Notes") for identified cyber security CSs, if available.

2. COPY of operator training lesson plans and/or operator training aids for identified cyber security CSs, if available.

3. Organizational chart for corporate and site personnel involved in establishing, overseeing, and maintaining the cyber security program.

4. Phone list for licensee personnel associated with cyber security and this inspection.

5. List of abbreviations and/or designators for plant systems.

D. Milestone Specific Documents

Provide a separate document list (in a table format) for each milestone, similar to:

Document No.	Title	Description	Rev
No. 1			
No. 2			
No. 3			
etc.			

1. MILESTONE 1

   a. LIST of all documents necessary to perform independent verification of the effective implementation of Cyber Security Milestone 1.

   b. COPY of policies, procedures, and instructions which established and implemented the CSAT team, and controls CSAT team functioning.

   c. LIST of CSAT members and their primary areas of responsibility.

   d. COPY of policies and procedures detailing qualification requirements for CSAT members.

   e. COPY of supporting documentation that demonstrates each CSAT member meets the requirements to fulfill their respective position on the team. For example, member resumes; evaluation of previous education and experience; training required by implementing procedures and supporting documentation which shows training was completed; or industry certifications.

   f. COPY of cyber security related training and/or lesson plans for CSAT members.

   g. COPY of cyber security related training records for CSAT members.

   h. COPY of training program for cyber security engineers (e.g., general population of engineers who are not CSAT members), such as cyber security general awareness training.

2. MILESTONE 2

   a. LIST of all documents necessary to perform independent verification of the effective implementation of Cyber Security Milestone 2.

   b. COPY of policies, procedures, and instructions which established, implemented, and controlled the process by which CSs were identified and documented.

   c. LIST of plant systems, annotated as to which systems were identified as Critical Systems (CSs), in accordance with CSP, Section 3.1.3.

   d. LIST of Critical Digital Assets (CDAs).

e. COPY of policies, procedures, or instructions which established, implemented, and/or controlled the process by which CDAs were identified and documented, in accordance with CSP, Section 3.1.3.

f. If a software tool or program was used to screen systems as part of the process to determine which systems should be designated as CSs using software logic (e.g., the software determines which options or questions should be evaluated next, based on the answer to the last question), then provide the documentation which demonstrates that the software program was adequately verified and validated for its specific usage to assess system characteristics and identify CSs.

g. If a software tool or program was used to screen digital assets as part of the process to determine which digital assets should be designated as CDAs using software logic (e.g., the software determines which options or questions should be evaluated next, based on the answer to the last question), then provide the documentation which demonstrates that the software program was adequately verified and validated for its specific usage to assess digital assets and identify CDAs.

h. LIST of digital test equipment and portable media associated with or used for target set CDAs.

3. MILESTONE 3

a. LIST of all documents necessary to perform independent verification of the effective implementation of Cyber Security Milestone 3.

b. COPY of policies, procedures, and documents which established and implemented the cyber defensive architecture, as described in CSP, Section 4.3.

c. Describe any differences between the defensive architecture as currently implemented and the description of the architecture in CSP, Section 4.3.

d. COPY of any tracking documents for defensive architecture items that are not yet installed or fully implemented, including due dates and schedules for full implementation.

e. Describe any interim or compensatory measures currently in-place, in lieu of full implementation.

f. Provide an overview of the cyber defensive architecture, preferably with overview level diagrams showing the various levels relative to the location of the subject deterministic one-way device.

g. Provide details of the implementation of deterministic one-way devices.

4. MILESTONE 4

a. LIST of all documents necessary to perform independent verification of the effective implementation of Cyber Security Milestone 4.

b. COPY of policies, procedures, and instructions which implemented the security control "Access Control for Portable and Mobile Devices," as described in Appendix D Section 1.19 of NEI 08-09, Revision 6.

c. COPY of implementing procedures and instructions for the scanning of portable media and digital test equipment on kiosks.

d. COPY of implementing procedures and instructions for the scanning of portable media and digital test equipment without using kiosks (e.g., for digital test equipment that can not be scanned using a kiosk).

e. COPY of policies, procedures, and instructions that describe what to do if a virus or malware is detected.

f. COPY of policy or program requirements, including implementing procedures and instructions, for the setup, maintenance, and updating of anti-virus and malware scanning/detection programs used for scanning of portable media (e.g., administrative controls for implementation of scanning kiosks).

g. COPY of any performed test and test results of scanning kiosks that verified or validated the functional capabilities of the kiosks to detect viruses and malware on portable media (e.g., whatever testing shows that the kiosk platform/system was ready for deployment).

h. COPY of any testing or assessment of in-house software installed and running on scanning kiosks.

i. COPY of training material or cyber security awareness literature distributed to plant staff associated with this security control.

5. MILESTONE 5

a. LIST of all documents necessary to perform independent verification of the effective implementation of Cyber Security Milestone 5.

b. COPY of policies, procedures, and instructions which implemented the requirements described in Appendix E Section 4.3 of NEI 08-09, Revision 6.

c. COPY of training materials and lesson plans for Insider Mitigation Cyber Related Tampering training of plant staff responsible for performing rounds to identify cyber related tampering.

d. COPY of training records for plant staff performing insider mitigation rounds.

e. COPY of records or logs which show insider mitigation rounds were performed, including any associated checklist or signoff sheets (three examples).

f. COPY of policies, procedures, and instructions for oversight of contractor personnel who work on CDAs.

6. MILESTONE 6

- Any documents requested for this milestone that contains safeguards information should be made available during the on-site Information Gathering Visit and not included on a CD (e.g., safeguards information should not be transmitted or sent to the Regional office).

- Any requested documents that are safeguards information should be added to the Group II document list, for use on-site during the information Gathering Visit.

a. LIST of all documents necessary to perform independent verification of the effective implementation of Cyber Security Milestone 6.

b. COPY of policies, procedures, and documents which were used to identify and document target set CDAs.

c. COPY of policies, procedures, and documents which were used to identify, document, and implement technical cyber security controls, in accordance with CSP, Section 3.1.6, for target set CDAs. (Only non-safeguards information)

d. COPY of policies, procedures, and documents which provide the basis for determining whether a CDA, whose function directly affects target set equipment or components, is designated as a non-target set CDA (e.g., basis for screening out a CDA as a target set CDA). (Only non-safeguards information)

e. If a software tool or program was used to screen CDAs as part of the process to determine which technical controls should be implemented for a CDA using software logic (e.g., the software determines which technical controls or questions should be evaluated next, based on the answer to the last question), then provide the documentation which demonstrates that the software program was adequately verified and validated for its specific usage to assess CDA vulnerabilities and identify appropriate controls.

f. Describe any differences between the technical cyber security controls as currently implemented and the controls required by CSP, Section 3.1.6, for target set CDAs. (Only non-safeguards information)

g. For target set CDA cyber security controls that are implemented, provide the procedures and instructions implementing the control. Common controls for all CDAs may be provided in a separate list with the procedures implementing each of them. (Only non-safeguards information)

h. For alternate controls that have been implemented, provide the documented basis for employing alternative countermeasures, and the procedures implementing the alternative measures. (Only non-safeguards information)

i. If operator or manual actions are used to protect target set CDA functions, then provide the verification and validation of feasible and timely implementation, communications capability is protected from effects of a cyber attack as needed, and associated training.

j. Where controls have been deemed unnecessary, provide the threat vector analysis supporting the conclusion that the threat vector does not exist. (Only non-safeguards information)

k. COPY of any tracking documents for technical cyber security controls that are not yet installed or fully implemented for target set CDAs, including due dates and schedules for full implementation. (Only non-safeguards information)

l. Describe any interim or compensatory measures currently in-place, in lieu of full implementation. (Only non-safeguards information)

7. MILESTONE 7

- Any documents requested for this milestone that contains safeguards information should be made available during the on-site Information Gathering Visit and not included on a CD for this document group (e.g., safeguards information should not be transmitted or sent to the Regional office).

- Any requested documents that are safeguards information should be added to the Group II document list, for use on-site during the information Gathering Visit.

a. LIST of all documents necessary to perform independent verification of the effective implementation of Cyber Security Milestone 7.

b. COPY of policies, procedures, and instructions which established and implement on-going monitoring and assessment activities as described in CSP, Section 4.4.

c. For all controls that are implemented, provide the objective evidence that the control is effective in accordance with CSP, Section 4.4.3.1. This may be combined with the documentation provided for Milestone 6. Documentation for common controls for all CDAs may be provided in a separate list with the procedures implementing each of them.

d. COPY of policies, procedures, and training for response to cyber security incidents.

e. COPY of policies, procedures, and instructions for handling and monitoring cyber security incident response.

f. COPY of policies, procedures, and instructions for performing vulnerability scans as described in CSP, Section 4.4.3.2.

g. COPY of any results for vulnerability scans or assessments that were performed for target set CDAs.

h. COPY of assessments which demonstrate the effectiveness of vulnerability scans and vulnerability assessments for target set CDAs.

i. COPY of policies, procedures, and instructions for performing vulnerability assessments for target set CDAs.

II. Information Requested during the Information Gathering Visit

- The documents requested below should be made available to the inspection team on the first day of the Information Gathering Visit.

- This document group is intended to include (1) CS and/or CDA specific information related to inspection samples which will be selected during the Information Gathering Visit, (2) milestone specific Safeguards Information, and (3) any updates to previously provided information.

- Safeguards Information is to be made available for inspectors use while on-site (not to be placed on CDs).

- Please provide the requested information (non-safeguards only) on three sets of CDs (searchable and hyper-linked, if possible).

1. Provide a presentation/discussion of the CSP, existing cyber security CSs, and associated CDAs.

2. Provide an overview discussion of the CSP, existing cyber security CSs, and associated CDAs.

3. Provide any updates to information previously provided.

4. Provide any documents that were previously requested, but were not available at the time that the previous data CD was provided.

5. MILESTONE 2

    a. Be prepared to provide a list of plant components, noting which components have been identified as CDAs.

    b. Physical Security Program target sets (safeguards information)

    c. LIST of target set CDAs (safeguards information)

6. MILESTONE 3

    a. Provide an overview walkdown of the cyber architecture within the plant, including safety, security, and emergency preparedness related CDAs.

7. MILESTONE 6

    a. Provide an overview and discussion of milestone activities for target set CDAs.

    b. COPY of policies, procedures, and documents which were used to identify, document, and implement technical cyber security controls, in accordance with CSP, Section 3.1.6, for target set CDAs (safeguards information).

c. COPY of policies, procedures, and documents which provide the basis for determining whether a CDA, whose function directly affects target set equipment or components, is designated as a non-target set CDA (e.g., basis for screening out a CDA as a target set CDA). (safeguards information)

d. For selected target set CDAs, provide documentation for each of the technical controls in Appendix D of NEI 08-09, Revision 6, and the results of reviews required under CSP, Section 3.1.6. (safeguards information)

e. Describe any differences between the technical cyber security controls as currently implemented and the controls required by CSP, Section 3.1.6, for target set CDAs. (safeguards information)

f. For target set CDA cyber security controls that are implemented, provide the procedures and instructions implementing the control. Common controls for all CDAs may be provided in a separate list with the procedures implementing each of them. (safeguards information)

g. For alternate controls that have been implemented, provide the documented basis for employing alternative countermeasures, and the procedures implementing the alternative measures. (safeguards information)

h. Where controls have been deemed unnecessary, provide the threat vector analysis supporting the conclusion that the threat vector does not exist. (safeguards information)

i. COPY of any tracking documents for technical cyber security controls that are not yet installed or fully implemented for target set CDAs, including due dates and schedules for full implementation. (safeguards information)

j. Describe any interim or compensatory measures currently in-place, in lieu of full implementation. (safeguards information)

8. MILESTONE 7

a. For the CDAs selected above, be prepared to produce documentation for each of the technical controls in Appendix D of NEI 08-09, Revision 6, and the results of immediate activities required under CSP, Section 4.4.

III. Information Requested to be Available On-site on the First Day of the Inspection

- The documents and information requested below should be made available to the inspection team on the first day of the on-site inspection.

- Safeguards Information is to be made available for inspectors use while on-site (not to be placed on CDs).

- Please provide the requested information (non-safeguards only) on three sets of CDs (searchable and hyper-linked, if possible).

    1. Provide any updates to information previously provided.

    2. Provide any documents that were previously requested, but were not available at the time.

IV. Information Requested to Be Provided throughout the Inspection

Copies of the list of questions/documents requested identified by the inspector and the status/resolution of the information requested (provided daily during the inspection to each inspector).