January 11, 2011

Mr. Jim Kay, Licensing Manager
AES Eagle Rock Enrichment Facility
400 Donald Lynch Boulevard
Marlborough, MA 01752

SUBJECT: GUIDANCE ON CLASSIFIED COMPUTER NETWORK CYBER SECURITY PLANS AND CONFIGUTATION MANAGEMENT CHANGE CONTROL

Dear Mr. Kay:

In a letter dated July 23, 2009, the U.S. Nuclear Regulatory Commission (NRC) indicated its acceptance of NEI 08-11, "Information Security Program Guidelines for Protection of Classified Material at Uranium Enrichment Facilities," which provides guidance for the protection of classified information, equipment, and technology and recommends the development and implementation of several programs and additional requirements. Section 3, "Specific Program Requirements," of NEI 08-11, contains the following guidance related to classified computer networks:

> Integrated computer networks that process, store, and transmit classified data must be accredited and approved by a Designated Approval Authority (DAA). Classified cyber security plans and their corresponding computer systems will be assessed in accordance with the agreements between the NRC and the U.S. Department of Energy (DOE). DOE, as the DAA, will conduct site audits, with NRC presence, and report the results to the enricher, as well as to the NRC. The NRC will authorize operation of the computer systems following approval and accreditation by the DAA.
>
> Each enricher's Standard Practice Procedures Plan (SPPP) will have a requirement for an accredited information technology (IT) plan. The IT plan will be updated as the DAA requirements change and the enricher will obtain NRC approval of any substantive changes to the plan. The SPPP should provide a plan-specific definition for "substantive changes." The definition will be consistent with Title 10 of the *Code of Federal Regulations* (10 CFR) 95.19.

If a plan-specific definition for "substantive changes" has not yet been provided, the enricher may not make any plan changes, substantive or non-substantive, without NRC approval. Additional guidance on substantive and non-substantive changes can be found in the enclosure to this letter.

Current enrichers should review this information for applicability to their facilities, as well as their vendors and contractors that possess or use classified matter and utilize classified computer networks.

In accordance with 10 CFR 2.390 of the NRC's "Rules of Practice," a copy of this letter will be available electronically for public inspection in the NRC Public Document Room or from the Publicly Available Records component of the NRC's Agencywide Documents Access and Management System (ADAMS). ADAMS is accessible from the NRC Web site at http://www.nrc.gov/reading-rm/adams.html (the Public Electronic Reading Room).

If you have any questions, please contact Brian Smith of my staff at 301-492-3137 or via email at Brian.Smith@nrc.gov.

Sincerely,

/RA/

Michael Tschiltz, Acting Director
Division of Fuel Cycle Safety
and Safeguards
Office of Nuclear Material Safety
and Safeguards

Docket No. 70-7015
License No. SNM-2015

Enclosure: As stated

cc: Mr. George Harper, P.E.
Vice President of Engineering
AES Eagle Rock Enrichment Facility
400 Donald Lynch Boulevard
Marlborough, MA 01752

In accordance with 10 CFR 2.390 of the NRC's "Rules of Practice," a copy of this letter will be available electronically for public inspection in the NRC Public Document Room or from the Publicly Available Records component of the NRC's Agencywide Documents Access and Management System (ADAMS). ADAMS is accessible from the NRC Web site at http://www.nrc.gov/reading-rm/adams.html (the Public Electronic Reading Room).

If you have any questions, please contact Brian Smith of my staff at 301-492-3137 or via email at Brian.Smith@nrc.gov.

Sincerely,

/RA/

Michael Tschiltz, Acting Director
Division of Fuel Cycle Safety
and Safeguards
Office of Nuclear Material Safety
and Safeguards

Docket No. 70-7015
License No. N/A

Enclosure: As stated

cc: Mr. George Harper, P.E.
AES Eagle Rock Enrichment Facility

ML103010413

OFFICE	UEB	UEB	UEB	NSIR
NAME	TBriley	WMoore	TNaquin	KEverly
DATE	10/26/10	11/4/10	11/4/10	11/30/10

OFFICE	UEB	FFLD	FCSS
NAME	AFrasier	BSmith	MTschiltz
DATE	12/06/10	1/07/11	1/11/11

OFFICIAL USE ONLY

January 11, 2011

Mr. Gary Sanford, Director
Quality and Regulatory Affairs
Louisiana Energy Services, L.P.
Eunice, NM 88231

SUBJECT: GUIDANCE ON CLASSIFIED COMPUTER NETWORK CYBER SECURITY PLANS AND CONFIGUTATION MANAGEMENT CHANGE CONTROL

Dear Mr. Cowne:

In a letter dated July 23, 2009, the U.S. Nuclear Regulatory Commission (NRC) indicated its acceptance of NEI 08-11, "Information Security Program Guidelines for Protection of Classified Material at Uranium Enrichment Facilities," which provides guidance for the protection of classified information, equipment, and technology and recommends the development and implementation of several programs and additional requirements. Section 3, "Specific Program Requirements," of NEI 08-11, contains the following guidance related to classified computer networks:

> Integrated computer networks that process, store, and transmit classified data must be accredited and approved by a Designated Approval Authority (DAA). Classified cyber security plans and their corresponding computer systems will be assessed in accordance with the agreements between the NRC and the U.S. Department of Energy (DOE). DOE, as the DAA, will conduct site audits, with NRC presence, and report the results to the enricher, as well as to the NRC. The NRC will authorize operation of the computer systems following approval and accreditation by the DAA.
>
> Each enricher's Standard Practice Procedures Plan (SPPP) will have a requirement for an accredited information technology (IT) plan. The IT plan will be updated as the DAA requirements change and the enricher will obtain NRC approval of any substantive changes to the plan. The SPPP should provide a plan-specific definition for "substantive changes." The definition will be consistent with Title 10 of the *Code of Federal Regulations* (10 CFR) 95.19.

If a plan-specific definition for "substantive changes" has not yet been provided, the enricher may not make any plan changes, substantive or non-substantive, without NRC approval. Additional guidance on substantive and non-substantive changes can be found in the enclosure to this letter.

Current enrichers should review this information for applicability to their facilities, as well as their vendors and contractors that possess or use classified matter and utilize classified computer networks.

In accordance with 10 CFR 2.390 of the NRC's "Rules of Practice," a copy of this letter will be available electronically for public inspection in the NRC Public Document Room or from the Publicly Available Records component of the NRC's Agencywide Documents Access and Management System (ADAMS). ADAMS is accessible from the NRC Web site at http://www.nrc.gov/reading-rm/adams.html (the Public Electronic Reading Room).

If you have any questions, please contact Brian Smith of my staff at 301-492-3137 or via email at Brian.Smith@nrc.gov.

Sincerely,

/RA/

Michael Tschiltz, Acting Director
Division of Fuel Cycle Safety
and Safeguards
Office of Nuclear Material Safety
and Safeguards

Docket No. 70-3103
License No. SNM-2010

Enclosure: As stated

cc: W. Padgett
Louisiana Energy Services

January 11, 2011

Ms. Julie Olivier
GE Hitachi Global Laser Enrichment
P.O. Box 780
3901 Castle Hayne Road
Wilmington, NC 28402

SUBJECT: GUIDANCE ON CLASSIFIED COMPUTER NETWORK CYBER SECURITY PLANS AND CONFIGUTATION MANAGEMENT CHANGE CONTROL

Dear Ms. Olivier:

In a letter dated July 23, 2009, the U.S. Nuclear Regulatory Commission (NRC) indicated its acceptance of NEI 08-11, “Information Security Program Guidelines for Protection of Classified Material at Uranium Enrichment Facilities,” which provides guidance for the protection of classified information, equipment, and technology and recommends the development and implementation of several programs and additional requirements. Section 3, “Specific Program Requirements,” of NEI 08-11, contains the following guidance related to classified computer networks:

> Integrated computer networks that process, store, and transmit classified data must be accredited and approved by a Designated Approval Authority (DAA). Classified cyber security plans and their corresponding computer systems will be assessed in accordance with the agreements between the NRC and the U.S. Department of Energy (DOE). DOE, as the DAA, will conduct site audits, with NRC presence, and report the results to the enricher, as well as to the NRC. The NRC will authorize operation of the computer systems following approval and accreditation by the DAA.
>
> Each enricher’s Standard Practice Procedures Plan (SPPP) will have a requirement for an accredited information technology (IT) plan. The IT plan will be updated as the DAA requirements change and the enricher will obtain NRC approval of any substantive changes to the plan. The SPPP should provide a plan-specific definition for "substantive changes." The definition will be consistent with Title 10 of the *Code of Federal Regulations* (10 CFR) 95.19.

If a plan-specific definition for “substantive changes” has not yet been provided, the enricher may not make any plan changes, substantive or non-substantive, without NRC approval. Additional guidance on substantive and non-substantive changes can be found in the enclosure to this letter.

Current enrichers should review this information for applicability to their facilities, as well as their vendors and contractors that possess or use classified matter and utilize classified computer networks.

In accordance with 10 CFR 2.390 of the NRC's "Rules of Practice," a copy of this letter will be available electronically for public inspection in the NRC Public Document Room or from the Publicly Available Records component of the NRC's Agencywide Documents Access and Management System (ADAMS). ADAMS is accessible from the NRC Web site at http://www.nrc.gov/reading-rm/adams.html (the Public Electronic Reading Room).

If you have any questions, please contact Brian Smith of my staff at 301-492-3137 or via email at Brian.Smith@nrc.gov.

Sincerely,

/RA/

Michael Tschiltz, Acting Director
Division of Fuel Cycle Safety
and Safeguards
Office of Nuclear Material Safety
and Safeguards

Docket No. 70-1113
License No. N/A

Enclosure: As stated

cc: Ms. Patricia Campbell/GLE
Mr. Chris Monetta/GLE
Mr. Jerald Head/GLE

January 11, 2011

Mr. Peter J. Miner, Director
Regulatory and Quality Assurance
USEC Inc.
Two Democracy Center
6903 Rockledge Drive
Bethesda, MD 20817-1818

SUBJECT: GUIDANCE ON CLASSIFIED COMPUTER NETWORK CYBER SECURITY PLANS AND CONFIGUTATION MANAGEMENT CHANGE CONTROL

Dear Mr. Miner:

In a letter dated July 23, 2009, the U.S. Nuclear Regulatory Commission (NRC) indicated its acceptance of NEI 08-11, "Information Security Program Guidelines for Protection of Classified Material at Uranium Enrichment Facilities," which provides guidance for the protection of classified information, equipment, and technology and recommends the development and implementation of several programs and additional requirements. Section 3, "Specific Program Requirements," of NEI 08-11, contains the following guidance related to classified computer networks:

> Integrated computer networks that process, store, and transmit classified data must be accredited and approved by a Designated Approval Authority (DAA). Classified cyber security plans and their corresponding computer systems will be assessed in accordance with the agreements between the NRC and the U.S. Department of Energy (DOE). DOE, as the DAA, will conduct site audits, with NRC presence, and report the results to the enricher, as well as to the NRC. The NRC will authorize operation of the computer systems following approval and accreditation by the DAA.
>
> Each enricher's Standard Practice Procedures Plan (SPPP) will have a requirement for an accredited information technology (IT) plan. The IT plan will be updated as the DAA requirements change and the enricher will obtain NRC approval of any substantive changes to the plan. The SPPP should provide a plan-specific definition for "substantive changes." The definition will be consistent with Title 10 of the *Code of Federal Regulations* (10 CFR) 95.19.

If a plan-specific definition for "substantive changes" has not yet been provided, the enricher may not make any plan changes, substantive or non-substantive, without NRC approval. Additional guidance on substantive and non-substantive changes can be found in the enclosure to this letter.

Current enrichers should review this information for applicability to their facilities, as well as their vendors and contractors that possess or use classified matter and utilize classified computer networks.

In accordance with 10 CFR 2.390 of the NRC's "Rules of Practice," a copy of this letter will be available electronically for public inspection in the NRC Public Document Room or from the Publicly Available Records component of the NRC's Agencywide Documents Access and Management System (ADAMS). ADAMS is accessible from the NRC Web site at http://www.nrc.gov/reading-rm/adams.html (the Public Electronic Reading Room).

If you have any questions, please contact Brian Smith of my staff at 301-492-3137 or via email at Brian.Smith@nrc.gov.

Sincerely,

/RA/

Michael Tschiltz, Acting Director
Division of Fuel Cycle Safety
and Safeguards
Office of Nuclear Material Safety
and Safeguards

Docket No. 70-7003, 70-7004
License No. SNM-7003, SNM-2011

Enclosure: As stated

cc: Mr. Terry Sensue, USEC Inc.

Substantive and Non-Substantive Changes

All licensees should document changes to their facility as part of configuration management. The rigor used to test, validate, and approve changes is directly related to the significance of the change and its impact to the operation of the system or the security requirements of the system. Changes, therefore, are described as substantive or minor, non-substantive. All substantive changes should be documented, tested, reviewed and approved. Minor, non-substantive changes should be documented and, to the extent possible, validated.

With regard to computer networks that process, store, and transmit classified data, substantive changes can be considered as those changes that, when made, affect the current operational security of a system. Examples of substantive changes include technology refreshments, operating system upgrades, device rebuilds that do not follow a documented baseline image, installation of new network devices, adding software not on an approved site list, significant replacement of hardware and/or software due to technical refresh, and significant network re-configuration actions.

Minor, non-substantive changes can be any changes that, when implemented, have little or no impact to the current operational status or security posture of the system. Examples of minor non-substantive changes include patching; updating antivirus signatures; upgrades to existing office products such as Microsoft Office, Adobe, etc. (defined by site); adding, updating, and removing users; adding software from an approved software list; replacement of a few components due to hardware/software failure as repair actions; and configuration change to a system component or a few components.