Page 01 of 64

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Remsburg, Kristy

From: Vrahoretis, Susan
Sent: Wednesday, October 31, 2012 12:44 PM
To: Vietti-Cook, Annette
Cc: Bavol, Rochelle; Bates, Andrew; Remsburg, Kristy; Niedzielski-Eichner, Phillip; Zimmerman, Jacob
Subject: FW: Guidance on Providing OUO to Congress
Attachments: NRC Policy for Handling, Marking, and Protecting SUNSI.pdf; MD 12.6 mark-up.pdf; 2010-04-27 guidance.pdf; 2005-10-26 guidance.pdf; 2004-0191scy - mark-up.pdf; Ignoring Perceived Security Concerns Regarding Jocassee Dam.pdf

Follow Up Flag: Follow up
Flag Status: Flagged

Hi, Annette,

We received this on Friday. It is related to other correspondence that the EDO is preparing a response to.

Thank you,

Susan

Susan H. Vrahoretis
Legal Counsel
Office of Chairman Allison M. Macfarlane
United States Nuclear Regulatory Commission
Office: O17D07
✉ E-mail: Susan.Vrahoretis@nrc.gov | ☎ Office: (301) 415-1834 |

From: Criscione, Lawrence
Sent: Friday, October 26, 2012 6:33 PM
To: Burrows, Sheryl; ODonnell, Edward; Salomon, Arthur; Sullivan, Randy; LaFranzo, Michael; Langstaff, Ronald; Lange, Walter; Thomas, James; NTEU, Chapter 208; Hearn, Peter; Iryll Robbins-Umel
Cc: Perkins, Richard; Mitman, Jeffrey; Galloway, Melanie; Boyce, Tom (RES); Sancaktar, Selim; Bensi, Michelle; Philip, Jacob; Circle, Jeff; Ferrante, Fernando; Pohida, Marie; Zoulis, Antonios; Chung, Donald; Wong, See-Meng; Vrahoretis, Susan; Zimmerman, Jacob; Wilson, George; Beasley, Benjamin; Coe, Doug; Zimmerman, Jacob; Correia, Richard; Ross-Lee, MaryJane; Pretzello, Andrew; Skidmore, Karen; Cardenas, Daniel; Ruland, William
Subject: Guidance on Providing OUO to Congress

Let me begin by saying I have been a NTEU member since 2010.

Attached is some of the disjointed guidance for "Official Use Only" information. In the email trail below is some of the history of this issue. I have not yet received answers to my four questions in one of the emails below to Dan Cardenas, but regardless of the answers specifically given to me for my specific situation, I believe that the NRC guidance on "OUO – SRI" could leave an employee with the impression that they cannot share Official Use Only information with Congress without meeting some undefined *"established need-to-know the information for conducting official business"*.

In 2005 one of the Resident Inspectors at Oconee Nuclear Station (ONS) noted a violation in ONS's failing to adequately control an access penetration through their flood wall surrounding their Standby Shutdown Facility (SSF). The penetration had been breached on August 13, 2003 to run a "temporary" power cable and was not restored until nearly

two years later (August 3, 2005). The violation issued by the resident inspector did not directly concern flooding protection but rather dealt with poor work practices that allowed a barrier breach to be forgotten about.

Duke Energy fought the violation. In defending his issuance of the violation, the resident inspector accidently stumbled across documentation suggesting that the flood wall around the Standby Shutdown Facility at Oconee is inadequately sized. This led to a White Finding against Duke Energy for knowing since 1993 that the five foot flood wall around the SSF would not be able to withstand the predicted 12 to 16 foot flood height that would occur were Jocassee Dam to fail. This information is all publicly available in the 2006-04-28 inspection report for ONS (ML061180451). The 2006 correspondence regarding the white finding is also publicly available (ML080780143 and ML063260282).

In defending their issuance of a White Finding, Region II eventually needed assistance from NRR. Once NRR became involved in 2007, all correspondence regarding the issue began being withheld from the public under the guise of "Official Use Only – Safety-Related Information" (OUO – SRI).

In 2007, there was probably very good reason for NRR to insist that the Jocassee Dam concerns be marked "OUO – SRI". I've attached a mark-up of SECY-04-0191 which contains the guidance NRR provided to their staff for "Handling of Sensitive Unclassified (Nonsafeguards) Information on Nuclear Power Reactors That Could Reasonably Be Expected to Be Useful to a Potential Adversary ". I've highlighted both guidance that supports the withholding of the Jocassee Dam information and guidance which supports the release of the Jocassee Dam information. In my opinion, in 2007 the weight of the guidance supports the WITHHOLDING of the information. However, I will note to you the statement:

> *It is also important to maintain an appropriate and realistic view about the added security assurance provided by the control of non-SGI information. The withholding of certain design or operational information may introduce a hurdle for potential adversaries during their planning of a malevolent act. The effectiveness of the hurdle, however, depends on the assumed level of sophistication, education, and knowledge of the adversaries. In some cases, it may be more appropriate to assess and, if necessary, revise a security program in recognition that the subject information is in the public domain.*

Particularly note: "**In some cases, it may be more appropriate to assess and, if necessary, revise a security program in recognition that the subject information is in the public domain**."

Although by 2007 this issue had been known to the NRC for 17 years (since February 1994), it had really only been on the "radar screen" for a year. So, at that point the guidance most applicable to the NRR staffers, in my opinion, was:

> *The control of information as part of an overall program to safeguard against the intentional release of radioactive materials needs to consider those threats for which the withholding of information might be helpful. The assessment is not limited to or even related to the design basis threat (DBT) but should consider the entire range of possible malevolent acts against a nuclear power reactor or other licensed activity. The assessments and evaluations are, at this point, based largely on staff judgments unless more detailed simulations or vulnerability assessments are available.*

Please note: "**unless more detailed simulations or vulnerability assessments are available**." It is my opinion it should be NRC policy that whenever important safety information is withheld from the public "*based largely on staff judgments*" then the staff should be required to initiate "*more detailed simulations or vulnerability assessments*". If the union agrees with this, then I would like their assistance (e.g. formally writing the congressional staffs) in pressuring the NRC to change the current policy. For five years we have been withholding a grave safety concern from the people of Oconee County, South Carolina based on informal staff judgments on the security of Jocassee Dam and – from the documents I have found – have made no attempt to do a detailed analysis of the vulnerability of the three Oconee reactors to a terrorist induced failure of Jocassee Dam. We owe the rate payers in Oconee County better than that for the millions of dollars they contribute to our salaries. I'm not proposing that every time something is withheld, it needs an assessment. Just the import safety concerns. I don't know how best to define "important" but, due to the current vulnerability Jocassee Dam poses to Oconee Nuclear Station, the reactors at ONS have a Core Damage Frequency ten

times greater than a typical US PWR and the probability of a major release is about 100 times greater than at a typical PWR. I believe you will agree with me that this qualifies as "important" enough to require a formal security assessment so that the safety concerns can hopefully be openly shared with the public.

When George Wilson first brought the Jocassee Dam issue to our attention in the Office of Nuclear Regulatory Research (RES) with an informal February 2010 memo requesting a Generic Issue on flooding due to dam failures, our first reaction was to discount his memo as being "sensational". We felt it was inflammatory and contained unsupported over dramatizations of the risks faced at Oconee. So under the guise of "pre-decisional" (but not "OUO – SRI") we withheld it from the public by not making it an official agency record. I neither agree nor disagree with the decision to not place George Wilson's memo in ADAMS; I'm merely bringing it up to demonstrate how our first impression in RES was to discount the Jocassee Dam issue. That was also likely the first and ultimately final impression in Region II and NRR when this issue first arose in 1994. And, given that it took them over 18 months to really get serious with Duke Energy, it was assuredly the first impression in NRR when the issue was again brought to their attention in late 2006.

On August 15, 2008, after being involved since late 2006, NRR sent a letter to Duke Energy requesting information on the vulnerability that Jocassee Dam poses to the reactors at Oconee (ML081640244). Although this letter was entirely about safety vulnerabilities, it was marked "OUO – SRI". The only place the word "security" occurs in this letter is in the "OUO – SRI" markings. Similar for the remaining correspondence from 2008-2012. To my knowledge, we have yet to look into the supposed security vulnerability posed to Jocassee Dam to actually determine if it is real.

I do not believe there is a credible security threat posed to Jocassee Dam. However, I have no training and experience which allows me to confidently make that determination, and I know there are many people at the agency who believe there is a security threat (hence the reason all the "OUO – SRI" documents are still marked as such). If the union believes that the correspondence between the NRC and Duke Energy should remain "OUO – SRI", then I would appreciate their assistance in formally analyzing the security threat posed to the reactors at ONS by Jocassee Dam. For example, I would like the union to write a letter to some congressional committees informing them of concerns of their members regarding unanalyzed security threats to Jocassee Dam and the need for Duke Energy to analyze those threats and possibly better guard the dam. Remember the NRC guidance from SECY-04-0191: "**In some cases, it may be more appropriate to assess and, if necessary, revise a security program in recognition that the subject information is in the public domain**". I believe the Jocassee/Oconee issue certainly falls into the "*some cases*" category of this quote requiring an assessment and possibly a revised security plan.

On June 22, 2010 we sent a Confirmatory Action Letter (CAL) to Duke Energy (ML101730329). Because "OUO – SRI" documents are not portion marked, I risk being accused of releasing "OUO – SRI" information if I quote from this 2010-06-22 letter. The actions we directed Duke Energy to take and the dates we gave them are certainly relevant to any discussion of this topic. Essentially, the CAL required Duke Energy to have adequate flooding protections in place by 2011-11-30. Note that this letter – regarding concerns about an inadequately sized flood wall leading to the flooding induced core meltdowns of three reactors and subsequent containment failures in the event of a Jocassee Dam failure – was sent 9 months prior to the 2011-03-11 tsunami overtopping the inadequately sized flood wall at Fukushima and leading to the flooding induced core meltdowns of three reactors and subsequent containment failures. Also note that the pre-Fukushima date by which Duke Energy was required to have adequate flood protections in place was 2011-11-30.

With regard to the "portion marking" comment in the above paragraph, I believe that the NRC policy of not requiring portion markings on "OUO – SRI" documents sets up bargaining unit employees to find themselves in the position I now find myself in for allegedly distributing "OUO – SRI" material. I believe that the guidance I highlighted in the attached document entitled "2010-04-27 guidance.pdf" should be followed with regard to portion markings. That is, if there is any paragraph on the page which does not contain "OUO – SRI" material, then the person designating the document as "OUO – SRI" should be required to portion mark all the "OUO – SRI" paragraphs. If the union agrees with this, then I would appreciate it if they would appeal to the EDO to require that portion markings be done when designating documents as "OUO – SRI".

Due to the similarity of the postulated Jocassee/Oconee accident to Fukushima, one would think that following the Fukushima accident Duke Energy would be under greater pressure to improve their flooding defenses at Oconee. Yet this was not the case.

On April 29, 2011 – a mere seven weeks after the Fukushima reactors melted down and we witnessed on television the explosions of the buildings housing their containments – Duke provided to the NRC a list of flooding defenses it was to take at Oconee to prevent a similar accident there (ML111460063). This list had originally been due on 2010-11-30 but we allowed Duke Energy to give themselves a six month extension (ML103490330). In their 2011-04-29 letter, Duke Energy extended the original 2011-11-30 due date to 30 months after the NRC and FERC reviewed and approved their construction plans. Assuming this review could happen instantaneously, that placed the new due date around 2013-11-30. More realistically the new post-Fukushima due date was now mid 2014. However, after GI 204 was accepted in December 2011, it was decided that the GI could be rolled into the Fukushima orders. This, in my opinion, was a good decision. But the due dates assigned to the Fukushima orders did not take into account pre-existing issues which had already been assigned due dates. So, as a result, Duke Energy's already delayed mid-2014 schedule was now extended to 2017. In a September 20, 2012 letter (ML12219A163) NRR, however, has "cracked the whip" and is insisting on a due date of no later than 2016 – that's 23 years after the vulnerability was first internally raised at Duke Energy, 22 years after the NRC was first made aware of it, 10 years after it re-surfaced, over 4 years beyond the 2011-11-30 due date given in the pre-Fukushima CAL, and 2 years beyond the approximate due date Duke Energy agreed to in its 2011-04-29 post-Fukushima correspondence.

As the Jocassee/Oconee issue wound its way through NRR in 2008-2010, there were dissenters who voiced opinions that NRR was not acting strongly enough or quickly enough. These dissenters mainly came from NRR's Division of Risk Assessment (NRR/DRA), which was task with determining just how risky a dam break was to the reactors at Oconee. In order to keep from stamping this email "OUO – SRI" I cannot mention exactly what the risk is, but as mentioned above the risk of core damage is about 10 times higher and the risk of a release about 100 times higher than at typical US PWRs. On April 6, 2009 Melanie Galloway, the then Deputy Director of NRR/DRA, submitted a Non-Concurrence form (ML091170104) in which she expressed concern that NRR was not taking the correct approach to the Jocassee/Oconee issue.

On January 10, 2011, Jeff Mitman submitted a Non-Concurrence form (ML110260443) in which he expressed concerns that the analyses being done by Duke Energy were overly "rosy" (my word, not his). If you want to know what was in Jeff's and Melanie's Non Concurrences, you can look them up in non-public ADAMS. I bring them up merely to show that all through this process there has been internal push-back from both NRR and RES. Some people who only have heard about Richard Perkins' letter to the IG and my letters to the chairman and Senator Lieberman make the uninformed assumption that we have not at first tried to address our concerns via our chain of command. Although it is true that I have not (as I will discuss below), it is not true that dissention on the Jocassee/Oconee issue has not been thoroughly vetted. Although Melanie's and Jeff's are the only formal Non-Concurrences (that I know of) on this issue, from conversation with people in NRR I know that there has been less formal – but equally forceful – dissentions expressed in meetings and through internal email correspondence.

Regarding the "OUO – SRI" markings, the screening report for GI-204 spent nearly a year in the review chain. The biggest hold up during the review was pressure from NRR to remove specific parts of the report – such as the quotation from the 2008-09-26 Duke Energy letter (ML082750106) regarding the timing of core damage and containment failures following a dam break at Jocassee which has since made it into Wikipedia – in favor of replacement with more general statements of the problem. Keep in mind that we are not talking about a report to the public; this was an internal NRC report from the RES staff to the GI-204 screening committee. Why would we want to withhold the 2008-09-26 Duke Energy assessment from our own NRC staff tasked with screening the Generic Issue on flooding due to upstream dam failures? I do not have an answer. If the 2009-09-26 assessment is really "*Information on Nuclear Power Reactors That Could Reasonably Be Expected to Be Useful to a Potential Adversary*" then so be it. But Bill Ruland and his fellow screening committee members are not "potential adversaries" – they are NRC staff. And the authors of the report felt strongly that the screening committee should have as strong a case as possible to make their decision.

The status of the "OUO – SRI" markings was debated in countless emails and meetings during 2011 and early 2012. RES staff won out and the GI 204 Screening Report survived the review process largely intact. In February 2012 a decision was made to redact from the public version of the report any information that ultimately originated in sources considered "OUO – SRI". Concerns were expressed to me by several co-workers that these redactions would lessen the impact of the report without providing any gain with regard to security.

Consider what was redacted from the report:

- The NRC estimated failure frequency for Jocassee Dam: this frequency was based on a study of dam failures solely due to natural phenomena (e.g. earthquakes, floods) or latent engineering/construction flaws. Sabotage, vandalism, terrorism, etc. did not factor into this estimated frequency. Although Dave Lochbaum might be interested in getting his hands on this estimated frequency, I doubt members of Al Qaeda really care.
- The Duke Energy 2008-09-26 timeline of how soon after the dam break the cores would melt and containment buildings fail: what is the argument for making this "OUO – SRI"? Is it that it gives the terrorists an insight into how to attack Jocassee Dam? Or is it that it gives the terrorists an idea of how vulnerable the reactors at ONS are to the flooding that would occur were Jocassee Dam to fail? If it's the latter, then consider what happened at Fukushima when the tsunami overtopped the inadequately sized flood wall there on 2011-03-11; you don't have to be a nuclear engineer to suspect that the reactors at Oconee would behave the same way were a "tsunami" from a dam break to overtop their inadequately sized flood wall. Although the fact that the Duke Energy predictions in their 2008-09-26 timeline closely match what occurred 2½ years later at Fukushima might be of interest to terrorists, I would argue that it is much more interesting to the public, the congress and the interveners because, in my estimation, the real vulnerability is not a terrorist induced dam break but rather a dam break due to natural disaster or human errors. Our guidance tells us that we should place sharing information with the public ahead of withholding it from terrorists when it is likely that it can be obtained or reasoned from publicly available sources. I might be giving them too much credit, but I believe terrorists organizations can tie a Jocassee Dam failure to the Fukushima tsunami without the aid of the 2008-09-26 Duke Energy letter.
- Any information indicating the proximity of a dam to a nuclear plant: do we think terrorists do not have access to Google Map?

From the redacted report it is obvious that there are significant concerns regarding a failure of Jocassee Dam and the resultant flood at the Oconee Nuclear Station. But what is not obvious is how long we have known about it and have avoided addressing it. What Al Qaeda needs to evaluate their targeting is located in the redacted report. What the Union of Concerned Scientists needs to evaluate our performance was redacted from the report.

Based on complaints I was hearing from my RES and NRR colleagues regarding the slow pace of approval of the GI-204 Screening Report and speculation from some of these same colleagues that the "OUO – SRI" markings were being mis-used, on February 29, 2012 I printed a copy of the unredacted GI-204 screening report (ML112430114). I also printed up some of the Duke Energy correspondence referenced in the screening report, some of the internal NRC memos and the Non-Concurrence packages of Ms. Galloway and Mr. Mitman. I highlighted the parts of the documents I thought were important and wrote notes on them. My New-Flex schedule provides for a 3-hour lunch break on Monday and Tuesday to allow me to swim at the Rockville municipal pool. My intention was to take the Red Line to Capitol Hill on Tuesday, March 6, 2012 (the day we were slated to publicly release the redacted version of the GI-204 screening report) over my long lunch and provide my documents to the House Committee on Energy and Commerce and to the Senate Committee on the Environment and Public Works. I was going to do this to make sure that the concerned congressional oversight committees were aware of the issues surrounding Jocassee Dam and Oconee Nuclear Station.

Many of my peers would criticize me for doing this without first exhausting all internal avenues.

I am a professional engineer and as such have a duty to my employer. It is expected of me that if I uncover a problem I am to bring it to my employer for resolution and am only to take it outside of my employer if I am unsuccessful in getting it addressed internally. In the past – in the US Navy, at Clinton Power Station and at Callaway Plant – I rigorously

pursued concerns internally through my chain of command even though it was often to the detriment of my career. I do not shy away from doing that, and would have preferred to done it with the Jocassee/Oconee issues if not for extenuating circumstances.

The most important circumstance is that GI-204 was nothing I was assigned to. I knew about the troubles because of complaints from my co-workers and from associates at NRR. But, in terms of my job, it was not really my business. For that reason I did not think it appropriate to go up my chain of command via the Open Door Policy or to use the Differing Professional Opinions process..

Another circumstance is timing. By February 2012, this issue was 18 years old in one since and nearly 6-years old in its current re-incarnation. Going through the chain of command is tedious and time consuming. Had I got involved in 2008 as an NRR employee, I probably would have used the Open Door Policy, Non-Concurrence process, and the Differing Professional Opinions process. But not only were these processes not meant for me as an outsider (i.e. someone not in any way associated with the issue from a standpoint of *conducting official business*), but these processes are not very effective and would have wasted a lot of time. A nuclear colleague (Bill Corcoran) has noted to me "*Our culture supports going through channels and eschews doing end runs. An effect of this is that those who control the channels have myriad ways of delaying and blocking valid concerns.*" His analysis pretty much sums up my thinking process better than I can. Experience tells me that if Melanie Galloway – a Deputy Division Director in NRR – was unsuccessful with her Non-Concurrence form, then I would not fare any better with an Open Door meeting.

And yet another circumstance is the "subservient" role that many people in the RES management view RES has to NRR. One of my chief concerns on this issue is that for 6 years NRR has focused on downplaying a problem they know to be wrong instead of actively trying to correct it. I did not see going through RES management as a viable option since I believed RES management would be hesitant to confront NRR. This, by the way, is not just an "assumption". It is fact borne out by Richard Perkins' 12 month ordeal in getting the screening report for GI-204 approved.

I never made it down to Capitol Hill on March 6th. On March 1, 2012 my wife was diagnosed with breast cancer and I drove home to Illinois the next morning. Due to the union negotiated benefits that make this the Best Place to Work in the Federal Government – Comp Time for Travel, New Flex Schedule, Credit Hours, Work From Home, Sick Leave for Serious Family Medical Conditions – and the generosity of Region III in letting me use a spare office, I spent most of the next six months in Illinois while my wife went through her various medical treatments. My only weeks working in Maryland during that time were once in April and once in July.

On either Monday July 9th or Tuesday July 10th I took the Red Line to Capitol Hill over my 3-hour lunch and dropped off the unredacted screening report and support documents with staffers on the Senate Committee on the Environment and Public Works and staffers on the House Committee on Energy and Commerce.

When I was in the navy, there were several instances when congressional offices toured our submarine. As part of the preparation for the visit, the officers would all get the same briefing. We were told that the congressman was cleared to see anything he asked for and go into any space he chose. His staff, however, needed to have the appropriate clearance level (which they always did) and needed to have a "Need to Know" (which was assumed as long as they were accompanying the congressman). This, as well as other briefings and training in the military and the nuclear industry, left me with the impression that classified – and by default, pseudo-classified OUO documents – could be shared with congressional offices. However, I did not know the exact statute until this morning.

This afternoon I met with my Branch Chief and Division Director concerning the release of "OUO – SRI" documents outside the NRC. During that meeting, I was informed that anything I sent to Congress needed to go through my supervisors and the Office of Congressional Affairs. The rationale for this was that they do not want to get blindsided by questions from a congressional office.

My Branch Chief and Division Director are reasonable people and I do not have a problem with, as a courtesy, involving them and the Office of Congressional Affairs any time in the future when I provide "OUO – SRI" material to a

congressional office. To be honest, I feel I was wrong to do it in the past. I chose expediency over courtesy and would not have appreciated that choice were I in their shoes. However, I do have a problem with this as a requirement. Not everyone I've worked for is as reasonable as my current Branch Chief and Division Director. And certainly in your time at the NRC all of you have at some point encountered supervision that you could not openly dissent with without it affecting your performance appraisal. I have never been a fan of secretively doing things, but for some employees it is necessary. We, as an agency, recognize this in that the Allegation Process we implement on the licensees is rooted in confidentiality.

Earlier today, it was brought to my attention that 5 USC §7211 guarantees a federal right to furnish information to members of Congress without interference. Regardless of whether or not this law applies to my having provided "OUO – SRI" documents to congressional staffers, I intend to, in the future, keep my Branch Chief and the OCA "in the loop". However, since I have, in the past, provided documents to congressional offices without informing OCA or my supervisors, I would like the union to inform me if 5 USC §7211 provided me a protected right as a federal employee to share the "OUO – SRI" documents regarding Jocassee Dam with the congressional offices with whom I shared them. Please note, that aside from my own issues, I believe that many people in the bargaining unit are not aware they have a protected right to address issues with congressional offices, and I believe that if this right exist then NTEU should ensure their members know of it and the basis for it.

I never heard from the congressional offices with whom I provided the documents in July.

In mid-September, Richard Perkins found out that the redactions to the GI-204 screening report had been requested through the Freedom of Information Act and that some of the redactions had been denied on the basis of being "OUO – SRI". Richard disagreed with the redactions and the way the NRC handles "OUO – SRI" and wrote a letter to the NRC Inspector General which was copied to his congressional Representative. He knew I had, in the past, been in contact with congressional offices concerning Region IV's response to a 2003-10-21 incident at Callaway Plant, and on September 14, 2012 he asked me if I could forward his letter along to any congressional office who I thought might be interested. I forwarded his letter and the unredacted screening report to about a dozen congressional offices. I also forwarded his letter along with the redacted screening report to the Union of Concerned Scientists. I did this because despite 6 years of internal pressure the NRC still did not have a coordinated plan to address the known safety concerns and the assumed security concerns regarding the Jocassee/Oconee issue.

On September 18, 2012 I sent a 19 page letter to Chairman Macfarlane and copied it to several congressional offices. Along with that letter, I forwarded some of the "OUO – SRI" documents concerning the Jocassee/Oconee issue. Although my letter contained quotes from "OUO – SRI" documents, I did not stamp it "OUO – SRI". And although my email contained information considered "OUO – SRI" and had "OUO – SRI" documents attached to it, I failed to designate my email "OUO – SRI". Because of these transgressions, my Branch Chief was directed to fill out a NRC Form 183 on me for performing an unauthorized release of restricted information. Aside from members of the NRC and from congressional staffers, my email was also sent to the US Special Counsel. Since my email and letter were not part of an OSC Form 12 disclosure, it is unclear if I was allowed to do this.

Between September 12, 2012 (when Richard Perkins told me he was writing the OIG) and last week, I have sent "OUO – SRI" to congressional offices on multiple occasions, usually at the request of committee staff who, as they read documents, requested other documents which the earlier documents referenced. Today, I was asked to provide a list of all such "unauthorized disclosures" to Mary Jane Ross-Lee and will be doing so on Tuesday.

In early October I was contacted by Jim Riccio of Greenpeace. He had in his possession the unredacted screening report and a copy of my September 18th email and letter to the NRC Chairman. He did not mention the references that were sent with that email, but I assume he has those as well. I informed Mr. Riccio that I could not speak to any of the technical aspects of the Jocassee/Oconee issue which the NRC considers "OUO – SRI" but that I could speak to the non-designated technical aspects, to my general opinion as to how NRR has been handling this issue, and to my specific opinions as to the motivations for the NRC's liberal use of "OUO – SRI".

Around October 18th (may have been one or two days earlier) while I was riding my bicycle Tom Zeller of the Huffington Post called me and asked me to comment on the NRC Public Affairs Office's statements regarding the Jocassee/Oconee issue. The statement Mr. Zeller read to me was something to the effect that Oconee Nuclear Station was adequately protected from all flooding events. My response to that was that the PAO was being dishonest. When the "They're being dishonest" quote appeared in his article, it was associated with a slightly updated NRC quote which, to my recollection, I still consider dishonest but was slightly more truthful than the original quote. Although it might be technically true that the flood protection at Oconee was adequate when regulated to their design basis, in the common public understanding of "adequate" we do not believe the flood protection is adequate otherwise we would not have spent the past four years (since August 15, 2008) berating Duke Energy to spend tens of millions of dollars upgrading their flooding defenses. Although the PAO was being "truthful" in a strict legal sense, in my opinion they were intentional misleading Mr. Zeller.

Last weekend, the Huffington Post posted the unredacted GI-204 screening report on the internet. I believe they got it from Greenpeace and they might even state as such in the article that they wrote that same weekend on the Jocassee/Oconee issue.

The Huffington Post also did an article on the Jocassee/Oconee issue the day Richard Perkins submitted his letter to the OIG. Following that article, I had a significant number of interactions with fellow NRC employees, congressional staffers, and non-NRC nuclear professionals regarding the need to keep the Jocassee/Oconee issue "from the terrorists". These discussions led me to question the security of Jocassee Dam. Although I believe the dam to not be a credible terrorist target, as I say above I do not have the background to credibly make that determination. So I wrote a five page letter to the Chairman of the Senate Committee on Homeland Security and Governmental Affairs requesting that his staff review whether or not adequate protection from terrorism has been evaluated for Jocassee Dam. I have attached that letter to this email. I do not consider my October 15, 2012 letter to contain "OUO – SRI" but would like you to be aware of it in case the NRC believes it does. At this point, no one at the NRC has told me I need to fill out a Form 183 for this letter. Note that, unlike my 2012-09-18 letter to the NRC Chairman, this letter intentionally did not reference any "OUO – SRI" information and for that reason I copied it to people outside of the US Government.

I've highlighted my requests of you in red. I apologize for the length of this email, but this is a long and involved issue. If each of you took an hour reading this letter, you will have each been making $40/hour in terms of the union dues I have paid in my short career at the NRC. I know you are not actually paid an extra $40 for your troubles, but I am nonetheless still voluntarily paying for it and I am interested in your assessments. Please call me at 573-230-3959 if you have any questions.

Thank you,

Larry
Lawrence Criscione, PE
Reliability & Risk Analyst
RES/DRA/OEGIB
573-230-3959

From: Lawrence Criscione [mailto:lscriscione@hotmail.com]
Sent: Friday, October 26, 2012 6:05 AM
To: Joe Carson
Subject: RE: Needing a Very Specific Reference Concerning Providing Information to Congress

Thanks Joe. I don't know if the 5 USC section 1213 applies since I have not yet submited an OSC Form 12 and I don't know if 5 USC 2302 applies since I have not yet been the recipient of any Prohibited Personnel Practices. I did not know about either of these statutes though and appreciate your bringing them to my attention.

Your reference to the Lloyd-LaFollette Act of 1912 led me to the Wikipedia page on it which led me to 5 USC § 7211 -

Employees' right to petition Congress:

> *The right of employees, individually or collectively, to petition Congress or a Member of Congress, or to furnish information to either House of Congress, or to a committee or Member thereof, may not be interfered with or denied.*

From: (b)(6)
To: lscriscione@hotmail.com
Subject: RE: Needing a Very Specific Reference Concerning Providing Information to Congress
Date: Thu, 25 Oct 2012 22:35:14 -0400

Lloyd-LaFollette Act of 1912. See 5 U.S.C. sections 1213(a)(1) and 2302(b)(8)(A) - if the info is not "prohibited by law or executive order" from public disclosure, it can be disclosed to Congress and everywhere else.

From: Lawrence Criscione [mailto:lscriscione@hotmail.com]
Sent: Thursday, October 25, 2012 10:02 PM
To: whistleblower411@yahoogroups.com; Joe Carson; Jim Riccio; David Lochbaum; Dave Lochbaum; Paul Blanch; David Collins; Louis Clark; scott@pogo.org; Tyson Slocum; Project On Government Oversight; Kay Drey; DR WILLIAM CORCORAN
Cc: Richard Perkins
Subject: Needing a Very Specific Reference Concerning Providing Information to Congress

I have always been told that providing information to Congress was a protected activity, but I don't know what law protects it and what restrictions that law has. Please see the email trail below for the context.

If you know the specific law that makes passing information to Congress a protected activity, please send me a link.

Thanks,
Larry Criscione
573-230-3959

From: Criscione, Lawrence
Sent: Thursday, October 25, 2012 9:37 PM
To: Cardenas, Daniel
Cc: Beasley, Benjamin; Coe, Doug; Ross-Lee, MaryJane; Pretzello, Andrew; Skidmore, Karen; ODonnell, Edward; Sullivan, Randy
Subject: Questions

Dan,

I have some questions regarding the guidance on the OIS SUNSI website and MD 12.6.

#1) In the attached document "2005-10-26 guidance.pdf" I've highlighted a sentence stating that portion markings are not required. However, in the document "2010-04-27 guidance.pdf" I've highlighted where it states:

> ***When is portion or page marking required?*** *On documents that may be released following redaction of sensitive information. If an entire page is not sensitive, place marking adjacent to the sensitive information.*

I am a big believer in portion markings. It frustrates me to no end that none of the 2008-2012 OUO correspondence between the NRC and Duke Energy regarding Jocassee Dam is portion marked. This correspondence clearly meets the instructions above for requiring that the documents be portion marked. That is, the overwhelming majority of the pages in the NRC/Duke correspondence have portions that are not sensitive and this NRC correspondence with a licensee concerning a serious safety concern should certainly *be released following redaction of sensitive information.*

Yet there are no portion markings. Which guidance is correct: the 2005-10-26 or the 2010-04-27 guidance? Should NRR's correspondence with Duke Energy from May 2010 through the present have been portion marked?

#2) On page 2 of the attached "NRC Policy for Handling Marking and Protection SUNSI.pdf" I have highlighted a paragraph on "Need-To-Know Access". This paragraph contains the words:

> *"...no person, including employees of the U.S. Government, NRC, ... may have access to SUNSI unless that person has an established need-to-know the information for conducting official business."*

I am unclear what exactly constitutes *"an established need-to-know the information for conducting official business."* Some of my co-workers (particularly Richard Perkins, but many others as well) expressed concern to me that flooding issues at Oconee Nuclear Station and Fort Calhoun were not being adequately addressed. Although it is my job (and the job of all NRC employees) to take allegations from licensees, I do not believe it is my job (i.e. *"conducting official business"*) to take allegations from my fellow NRC co-workers. Nonetheless, I reviewed some of the source documents regarding Jocassee Dam because I was concerned with the opinions I was hearing expressed from my co-workers. It was not my job to review these documents. Most of the review of these documents occurred after normal working hours, including times when – although allowed to be in the office or on Citrix – I am not allowed to formally work (i.e. beyond 8 pm, Sundays, while using annual leave/credit hours). Since I was reviewing this information on my own time and not *"for conducting official business"*, was I violating the "Need-to-Know".

Although I have only shared SUNSI with *"employees of the U.S. Government"*, I am not certain all of them had *"an established need-to-know the information for conducting official business"*:

- Does a staffer on the Senate Committee on Homeland Security & Governmental Affairs have *"an established need-to-know the information for conducting official business"*? If he does, must I send him through the Office of Congressional Affairs? Am I violating "Need-to-Know" by directly sending him references he requested?
- Does the intern for Representative Duncan of South Carolina's 3rd congressional district have *"an established need-to-know the information for conducting official business"* when she is not investigating any matter for a congressional oversight committee and I am merely copying her as a courtesy to keep her representative abreast of a concern regarding a nuclear plant in his district?
- Does the Office of the Special Counsel have *"an established need-to-know the information for conducting official business"* when the information is not being formally submitted with an OSC Form 12?
- Does the Downstate Director (i.e. Springfield, IL office chief) of Senator Durbin have *"an established need-to-know the information for conducting official business"* when I am merely meeting with him to get his advice as to whether or not my senator would be willing to write the NRC Chairman regarding the NRC's SUNSI policies?

#3) Assuming that the US Special Counsel or a congressional staffer has *"an established need-to-know"*, I am uncertain as to what is required by the "Access" requirements on page 5 of Part II of MD 12.6. Prior to sharing SUNSI with the US Special Counsel or congressional staffers, before providing the information must I first consult the three parties listed in MD 12.6:

- *NRC office originating the information*
- *Office that has primary interest in the information*
- *Source from which the information was derived*

#4) If I am writing a letter regarding how the Office of Nuclear Reactor Regulation is inappropriately stamping safety-related correspondence as "Security-Related Information", and if I am sending that letter to the US NRC Chairman and copying it to concerned congressional offices, and if I do not believe that marking the *letter is essential to ensure proper handling and to ensure all persons having access* to the letter *will be aware that* it (1) *must not be publicly released* and (2) *must be distributed only to those who have a need-to-know to conduct official business*, then am I in violation of MD 12.6 because I did not stamp the letter "Official Use Only – Security-Related Information"?

I was asked by a congressional staffer last month whether I believed the "Security-Related Information" stamps were hindering the open discussion of the Jocassee Dam/Oconee issue amongst the NRC staff. His concern was based on the fact that some of NRR's Jocassee Dam correspondence contain the stamp "Limited Internal Distribution Permitted". My answer to him was that, although I believed these stamps were inappropriately keeping a serious safety concern from public scrutiny, these markings were not in any way hindering the professional internal discussion of concerns regarding Jocassee Dam. Based on what I have read in MD 12.6 tonight, I do not know if I still agree with that answer. When possible, I would like to meet with you regarding the four questions above. Also, I have had people within the NRC request to see my 2012-09-18 letter to the chairman but I have been unwilling to share it with anyone since being told I was violating SUNSI guidance by not properly stamping it OUO – SRI. I would like to review that letter with you and get your assessment as to how it should be stamped.

R,

Larry

From: Criscione, Lawrence
Sent: Thursday, October 25, 2012 5:50 PM
To: Cardenas, Daniel
Subject: RE: Information Release

The version of MD 12.6 that is linked to in the SUNSI website is from December 20, 1999. Is this the version I am supposed to review or is there a more current revision?

From: Cardenas, Daniel
Sent: Thursday, October 25, 2012 5:39 PM
To: Criscione, Lawrence
Cc: Beasley, Benjamin; Coe, Doug; Ross-Lee, MaryJane; Pretzello, Andrew; Skidmore, Karen; ODonnell, Edward; Sullivan, Randy
Subject: Re: Information Release

Larry-

If you have read and understand the SUNSI guidance, then a meeting may not be necessary. I will contact you if a meeting is necessary. In regards to transmission of SUNSI outside the NRC, please contact your supervisor as identified in MD 12.6 and follow applicable guidance located on the OIS SUNSI website.

Regards.

Dan
~ Sent from an NRC Blackberry ~

Daniel Cardenas, Chief
Facilities Security Branch
Division of Facilities and Security
Office of Administration
U. S. Nuclear Regulatory Commission

Office Email: Daniel.Cardenas@nrc.gov
Office Number: (301) 415-6184
Cell Number: (b)(6)
Fax Number: (301) 415-5132

From: Criscione, Lawrence
To: Cardenas, Daniel
Cc: Beasley, Benjamin; Coe, Doug; Ross-Lee, MaryJane; Pretzello, Andrew; Skidmore, Karen; ODonnell, Edward; Sullivan,

Randy
Sent: Thu Oct 25 17:31:31 2012
Subject: RE: Information Release

Daniel,

My Outlook calendar is up to date through the end of the year. I should be able to review MD 12.6 and the other guidance by tomorrow morning.

The only personnel outside the NRC to whom I have provided "Official Use Only – Security Related Information" are either with the Office of the Special Counsel, staffers of US Senators or staffers of members of the US House of Representatives. I will not release any additional information to the Office of the Special Counsel or to members of the US Congress until I have met with you.

Please send me a copy of the NRC Form 183 mentioned below so that I may review it prior to our meeting.

Is my union steward allowed to accompany me to the meeting?

V/r,
Larry Criscione
573-230-3959

From: Cardenas, Daniel
Sent: Thursday, October 25, 2012 5:01 PM
To: Criscione, Lawrence
Cc: Beasley, Benjamin; Coe, Doug; Ross-Lee, MaryJane; Pretzello, Andrew; Skidmore, Karen
Subject: Information Release
Importance: High

Mr. Criscione-

I have received a NRC Form 183 "Report of Security Incident" indicating that you have released information (Official Use Only – Security Related Information, etc) to personnel outside of the NRC. This release of information must "stop" immediately. The guidance for handling Sensitive Unclassified non-Safeguards Information (SUNSI) is identified in MD 12.6 and on the OIS webpage. Please see the following link, which provides detailed information on the handling of this type of information.

(b)(7)(F)

If you have released any other information, you must cease these activities, and report the releases to the Director, Division of Facilities and Security.

Please schedule a time to discuss this matter with me.

Regards.

Daniel Cardenas
Chief, Facilities Security Branch
Division of Facilities and Security, Office of Administration

Location: T6-E31
Office Email: Daniel.Cardenas@nrc.gov
Office Number: (301) 415-6184
NRC Blackberry: (b)(6)
NRC Fax: (301) 415-5132

NRC Policy For
Handling, Marking, and Protecting
Sensitive Unclassified Non-Safeguards Information

A. Purpose and Scope

This policy is issued to ensure that sensitive unclassified non-safeguards information (SUNSI) is properly handled, marked, and adequately protected from unauthorized disclosure.

"SUNSI" means any information of which the loss, misuse, modification, or unauthorized access can reasonably be foreseen to harm the public interest, the commercial or financial interests of the entity or individual to whom the information pertains, the conduct of NRC and Federal programs, or the personal privacy of individuals.

The various categories of SUNSI have been organized into the following seven groups:

- Allegation information
- Investigation information
- Security-related information
- Proprietary information
- Privacy Act information
- Federal-, State-, foreign government-, and international agency-controlled information
- Sensitive internal information

To the extent that requirements under a section for a particular SUNSI group were already stipulated in a statute, regulation, or other directive, the requirements have been incorporated into this policy. The requirements set forth in this policy and procedures for handling allegation information come from Management Directive (MD) 8.8, "Management of Allegations." The requirements for the handling of Privacy Act information come from the Privacy Act of 1974, as amended, and MD 3.2, "Privacy Act." The requirements for marking incoming confidential commercial or financial (proprietary) information come from 10 CFR 2.390.

When more than one SUNSI group applies to information, the most restrictive handling requirement of the applicable groups should be applied.

B. Applicability

NRC employees, consultants, and contractors are responsible for ensuring the procedures specified in this announcement are followed to protect SUNSI. The use of the word "contractors" includes subcontractors.

C. Handling Requirements for SUNSI

1. Web Address for Handling Requirements

The handling requirements for SUNSI are published on the NRC internal Web site at http://www.internal.nrc.gov/sunsi/. The Web site contains detailed requirements for each of seven SUNSI groups in the following fourteen areas.

a. Applicable document categories
b. Authority to designate
c. Access
d. Marking
e. Cover sheet
f. Reproduction
g. Processing on electronic systems
h. Use at home
I. Use while traveling or commuting
j. Physical copy transmission
k. Electronic copy transmission
l. Storage
m. Destruction
n. Decontrol authority

2. Change requests

SUNSI handling requirements will be maintained and updated as needed at the SUNSI Web site. Changes will be announced to the NRC staff.

Requests to add additional document categories to a SUNSI group and other proposed changes should be submitted in writing to the Director, Information and Records Services Division, Office of Information Services. The request should state specifically where the addition or change should be made and a justification why the addition or change is needed.

D. Generally Applicable Requirements

1. Marking

Each document containing SUNSI must be properly and fully marked when such markings are required for the particular SUNSI group. (See item 4, Marking, in the SUNSI group handling requirements http://www.internal.nrc.gov/sunsi/.)

2. Need-To-Know Access

A security clearance is not required for access to SUNSI. However, except as the Commission may otherwise authorize, no person, including employees of the U.S. Government, NRC, an NRC licensee or certificate holder, or an employee, agent, or contractor of a license applicant may have access to SUNSI unless

that person has an established need-to-know the information for conducting official business.

If doubt exists in any particular case whether it is proper to grant access to SUNSI originating from outside the NRC, NRC contractors, or NRC licensees or applicants, consult with the originating party, the party responsible for the information, or other source from which the information is derived.

3. Ensuring legible markings on copies

All copies must clearly show the protective markings on the original document. Markings on documents submitted for reproduction should be in black or red and dark enough to be reproduced legibly.

4. Packaging SUNSI for Transmission

Material used for packaging SUNSI for physical transmission must be opaque and of such strength and durability as to provide secure protection for the document in transit, prevent items from breaking out of the container, and facilitate the detection of any tampering with the container.

5. Profiling SUNSI in ADAMS

When a document containing SUNSI is authorized to be entered into the Agencywide Documents Access and Management System (ADAMS), personnel entering the document must ensure that one of the sensitive values (Sensitive or Sensitive-Copyright, as appropriate) is marked in the "Document Sensitivity" profile property and that the "Availability" profile property is marked as "Non-Publicly Available." Identifying the appropriate document sensitivity and availability along with the markings on the documents will aid in protecting SUNSI. It will also alert staff to the sensitivity of the document when it is requested under FOIA or the Privacy Act, thus ensuring that the document is properly reviewed under FOIA and Privacy Act exemptions standards.

6. Removal of Markings

Normally a document will retain its markings until the agency decides that the document will be made public either on its own discretion, or in response to a Freedom of Information Act request. Before releasing a document with a SUNSI marking, the marking on the copy to be released should preferably be blackened out, or at a minimum, marked through in such a way that it conveys that the marking is no longer applicable to the document. This should be done on each page containing a marking.

7. Inadvertent or Unauthorized Release of SUNSI

Whenever SUNSI is inadvertently released or disclosed by the NRC or its contractors, the office director must promptly inform the Executive Director for Operations (EDO) and the Office of the Inspector General (OIG) in accordance with MD 3.4, "Release of Information to the Public."

8. Release of Information to the Public

Each document considered for routine release to the public by the agency must be reviewed to determine whether the document is releasable under NRC policy (See MD 3.4, "Release of Information to the Public") including application of screening criteria for determining if information should be withheld from public disclosure because it could reasonably be expected to be useful to a potential adversary. (See http://www.internal.nrc.gov/NRC/Guidance/index.html.) Each document requested by the public via the Freedom of Information Act or Privacy Act must be reviewed to determine whether the document, or part thereof, is releasable or is exempt from public disclosure. (See MD 3.1, "Freedom of Information Act" and MD 3.2, "Privacy Act.")

The presence or absence of cover sheets or markings as "Allegation Information," "Investigation Information," or similar markings, does not determine whether a document may be withheld from the public. Whenever an NRC employee has a question regarding the releasability of information, the employee should consult with the employee's supervisor or—

- The Information and Records Services Division (IRSD), Office of Information Services (OIS) if a request for information involves the Freedom of Information Act (FOIA) or the Privacy Act. (See MD 3.1, "Freedom of Information Act" and MD 3.2, "Privacy Act.")
- The Office of Enforcement (OE) regarding allegation information.
- The Office of Investigations (OI) regarding OI investigation information.
- The Office of the Inspector General (OIG) regarding OIG investigation information.
- The Office of Nuclear Reactor Regulation (NRR) or the Office of Nuclear Material Safety and Safeguards (NMSS), as appropriate, on whether a document contains 10 CFR 2.390(d)(1) information.
- The Office of the General Counsel (OGC), or appropriate regional counsel, on legal questions.

Other Government and International agencies should be consulted before documents bearing restrictive markings or containing SUNSI of primary interest to them are released to the public.

9. "No Comment" Policy for SUNSI

Should SUNSI appear in the public domain (e.g. newspapers) prior to the agency's official release of that information, and should an NRC employee be contacted by an organization outside of the agency to confirm or deny either the accuracy or sensitivity of the released information, NRC employees should respond to such a request with a "no comment" statement. If an NRC employee has any questions about how to handle a request for comment about an

unauthorized release of SUNSI, the employee should consult with the employee's supervisor or the originator of the information.

10. Security Preparations Required for Hearings, Conferences, or Discussions

NRC personnel, NRC consultants, NRC contractor personnel, and others (e.g., bidders) who arrange or participate in hearings, conferences, or discussions (see MD 3.5, "Attendance at NRC Staff Sponsored Meetings") involving SUNSI shall—

- Ensure before a hearing, conference, or discussion that participating personnel are identified and are authorized to have access to the information to be discussed.
- Inform participating personnel that the specific information they will receive is SUNSI and advise them of the protective measures required.
- Ensure that no discussion takes place that is audible or visible to persons not authorized access to the information.

Part II

Protection and Control of Sensitive Unclassified Information

Information Originated by NRC, NRC Contractors, or NRC Licensees (A)

The procedures set forth in this section apply to Safeguards Information (SGI), Official Use Only, and Proprietary information.

Access (1)

NRC personnel and NRC contractor employees shall furnish sensitive unclassified information to only those persons who need the information for the conduct of official business. (a)

If doubt exists as to whether it is proper to furnish information in any particular case, NRC personnel and NRC contractor employees shall consult the—(b)

- Originating office (If the information was originated by a contractor or a licensee, the originator or the NRC office administering the contract or license must be consulted.) (i)
- Office that has primary interest in the information (ii)
- Source from which the information was derived (iii)

If SGI is involved, NRC personnel or NRC contractor employees shall consult the Office of Nuclear Material Safety and Safeguards and the Office of Nuclear Reactor Regulation. (c)

If Proprietary or Official Use Only information is involved, NRC personnel or NRC contractor employees shall consult the—(d)

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

Access (1) (continued)

- NRC office originating the information (i)
- Office that has primary interest in the information (ii)
- Source from which the information was derived (iii)

An access authorization (security clearance) is not required for access to SGI or other sensitive unclassified information. However, the requirements of 10 CFR 73.57 mandate an FBI fingerprint check be conducted for access to SGI at a power reactor facility. (e)

No person may have access to SGI unless the person needs the information to conduct official business and the person is—(f)

- An employee, agent, or contractor of an applicant for a license, of an NRC licensee, of the NRC, or of the United States Government (i)
- A member of a duly authorized committee of the Congress (ii)
- The Governor of a State or his or her designated representative (iii)
- A representative of the International Atomic Energy Agency (IAEA) engaged in activities associated with the U.S./IAEA Safeguards Agreement who has been certified by the NRC (iv)
- A member of a State or local law enforcement authority that is responsible for responding to requests for assistance during safeguards emergencies (v)
- An individual to whom disclosure is ordered in accordance with 10 CFR 2.744(e) in connection with a domestic licensing proceeding (vi)

The office director or the regional administrator responsible for the document may authorize additional distribution of SGI related to activities conducted under the license. The individuals specified in the preceding list are normally considered to be trustworthy in view of their employment status. However, some discretion should be used in granting access if there is any indication that the proposed recipient would be unwilling or unable to provide the protection prescribed for SGI. (g)

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

When Information Is Marked (2)

Documents (including drafts and worksheets), other than for Official Use Only that contain sensitive unclassified information and require marking, must be marked upon origination.

SGI Documents (a)

Documents (including drafts and worksheets) known to contain SGI that are not so marked must be marked accordingly by persons authorized to designate information as "Safeguards Information."

- Documents dated before January 20, 1981, need not be marked until they are withdrawn from the files. (i)
- Documents dated before January 20, 1982, and clearly marked as 10 CFR 2.790(d) to indicate that they contain SGI must be secured as SGI without the alteration of their marking until they are withdrawn from the files for any reason. When withdrawn, these documents must be marked in accordance with this part. (ii)

Official Use Only Documents (b)

A document that contains information for Official Use Only must be marked when the originator believes that marking is essential to ensure proper handling and to ensure that all persons having access to the record will be aware that the—

- Document must not be publicly released. (i)
- Document must be distributed only to those who have a need-to-know to conduct official business. (ii)

Conditional Release Documents (c)

Some NRC documents may be released to the public when particular conditions have been met (e.g., a particular period of time has elapsed, a particular event has occurred, or an agency position has been officially approved). These documents are subject to conditional release and should be protected as Official Use Only until the specific condition has been met. While physical marking of conditional release documents may not be appropriate and is not required, the use of cover sheets marked "Official Use Only" is encouraged to facilitate their protection until they meet the condition for public release.

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

When Information Is Marked (2) (continued)

Proprietary Information Documents (d)

Documents received by NRC or NRC contractors that contain or are said to contain Proprietary information but that are not marked must be marked when marking is essential to ensure proper handling and to ensure that all persons having access to the information will be aware that the—

- Information must not be publicly released. (i)
- Information must be distributed only to those who have a need-to-know to conduct official business. (ii)

How Information Is Marked (3)

Safeguards Information (a)

At the time it is determined that a document contains SGI, originators must place the name, title, organization, signature, and date of the individual authorized to make an SGI determination and who has determined that the document contains SGI in the lower right corner of the face of the original document, as indicated in Exhibit 3 of this handbook. If the originator or approver of the document is the person authorized to make the determination and signs the document, that signature is sufficient. The signature in either case must appear on the face of the original copy of the document. Other copies may have a facsimile signature or a typed name. (i)

For a document containing SGI, originators must place the marking "SAFEGUARDS INFORMATION" conspicuously at the top and bottom of the page. Originators also must place the marking "Violation of protection requirements for SAFEGUARDS INFORMATION subject to CIVIL and CRIMINAL penalties" in the lower left corner of the face of the document. (ii)

Official Use Only (b)

Originators must place the marking "OFFICIAL USE ONLY" at the top and bottom of the page on the face of each document containing information for Official Use Only when that marking is required to

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

How Information Is Marked (3) (continued)

ensure proper handling. The marking "LIMITED INTERNAL DISTRIBUTION PERMITTED" must be placed in the lower left corner of the face of the document.

Proprietary Information (c)

Originators must place the words "PROPRIETARY INFORMATION" at the top and bottom of the page on the face of each document containing or said to contain Proprietary information.

Multiple Page Documents (d)

The "SAFEGUARDS INFORMATION, OFFICIAL USE ONLY," or "PROPRIETARY INFORMATION" markings must be placed at the top and bottom of—

- The outside of the front and back covers, if any (i)
- The title page, if any (ii)
- The first page of text, if there is no front cover or title page (iii)
- The outside of the back page, if there is no back cover (iv)
- Each page of a document containing sensitive unclassified information (v)

Portion-Marking (e)

Portion-marking is accomplished by clearly indicating the portions (e.g., titles, paragraphs, subjects, or pages) that contain sensitive unclassified information by placing the appropriate abbreviation (e.g., "SGI") in parentheses at the beginning or end of the portion.

Sensitive Unclassified Information (i)

Portion-marking is required for sensitive unclassified information when—

SUNSI Handling Requirements

Security-Related Information

printable version (pdf)

Table of Contents

What's New in SUNSI? (Updated Handling Requirements for Investigation Information)
SUNSI Policy and Procedures
Inadvertent or Unauthorized Release of SUNSI
Marking SUNSI in Electronic Formats
Frequently Asked Questions
SUNSI Training
Contact SUNSI.Resource@nrc.gov

APPLICABLE DOCUMENT CATEGORIES

- 10 CFR 2.390 Information
- Licensee-submitted information that may qualify as Critical Infrastructure Information as defined by other agencies including –

  - Critical Energy Infrastructure Information (CEII) – Federal Energy Regulation Commission (FERC)*
  - Sensitive Security Information (SSI) – Transportation Security Administration (TSA)*

- Information that could be useful, or could reasonably be expected to be useful to a terrorist in a potential attack that does not qualify as Safeguards or Classified Information (see Staff Guidance for Screening Documents that Could be Useful to a Terrorist)
- Sensitive Homeland Security Information – Department of Homeland Security (DHS) to define

* See other Federal-, State-, Foreign Government-, and International Agency-Controlled Information for their requirements (see) .

top

AUTHORITY TO DESIGNATE

NRC-Originated Information: The originator proposes and the signer approves designation.

Information Received by NRC: The office principally responsible for the information.

top

ACCESS

Who may have access?	NRC personnel or NRC contractor employees who need to know the information to perform their official duties.

top

MARKING

What documents should be marked?	Mark all pages of all documents.
Who may authorize document marking?	Originator, supervisor, or principal recipient.
How should a document	**NRC-Generated Documents:** Mark the top and bottom of each page -

be marked?	• **"Official Use Only – Security-Related Information."** **Documents Generated by Licensees, Applicants, Contractors or Other Outside Persons/Organizations Subject to NRC Jurisdiction:** Mark the top of each page - • **"Security-Related Information – Withhold Under 10 CFR 2.390."**
When is portion or page marking required?	On documents that may be released following redaction of sensitive information. If an entire page is not sensitive, place marking adjacent to the sensitive information.
COVER SHEET	
When should a cover sheet be used?	Not required. **Note:** Use of the green "Official Use Only" cover sheet has been discontinued.
What cover sheet is used?	Not applicable. top
REPRODUCTION	
How many copies may be made?	No restriction unless stated on the document; reproduction is limited to the number of copies needed for official use. Copies must clearly show the original markings. **Note**: Where restrictions are imposed on reproduction, the employee must also ensure that there are no non-authorized copies residing in electronic systems, such as on the network drive, local hard drive, or a floppy drive. top
PROCESSING ON ELECTRONIC SYSTEMS	
On what information systems may the document be processed?	NRC LAN and other systems accredited under MD 12.5, "NRC Automated Security Program."
Is encryption required while data is at rest?	Yes. Please follow the policy outlined in Yellow Announcement no. 157. http://www.internal.nrc.gov/announcements/yellow/2008/2008-157.html
May the information be processed in ADAMS?	Security-Related Information may be entered into the ADAMS Main Library and must be profiled as Non-Publicly Available and Sensitive. Assign access rights to user groups with a need to access the information to perform their official duties. ADAMS Sensitivity Code: A.3 – Sensitive-Security-Related – Periodic Review Required
USE AT HOME	
May I use the document at home?	Yes. Abide by the following requirements: • Employees are prohibited from routinely using, handling, or storing the information at their residences. Occasional use at an employee's residence requires approval of the employee's immediate supervisor or above. • To ensure that the information is not viewed or accessed inadvertently or willfully by a person not authorized access, the employee must ensure that the information cannot be seen by a family member, guest, or any other individual who is not authorized access. • All employees, including the staff and contractors, are prohibited from installing P2P software on agency computers without the explicit written approval of an agency Designated Approving Authority. In addition, employees are prohibited from processing SUNSI on home computers unless connected to and working within CITRIX, the NRC Broadband Remote Access System. Employees are prohibited from downloading or storing SUNSI to the hard drive of a home computer when connected to and working

	within CITRIX. Employees are also prohibited expressly from processing SUNSI on home computers even when an encrypted floppy disk, CD, DVD, or thumb drive is the storage media. Employees who work at home must perform electronic processing of SUNSI on either (1) a home computer within the virtual environment provided by the agency through CITRIX or (2) an NRC-issued laptop with NRC-approved encryption software.
May I use the information at home under the NRC Flexible Workplace Program?	Yes. Abide by the following requirements: • If you are approved to work at home under the NRC Flexible Workplace Program, use in accordance with standards set forth in NRC Form 624, Flexible Workplace Program Participation Agreement. • To ensure that the information is not viewed or accessed inadvertently or willfully by a person not authorized access, the employee must ensure that the information cannot be seen by a family member, guest, or any other individual who is not authorized access. • All employees, including the staff and contractors, are prohibited from installing P2P software on agency computers without the explicit written approval of an agency Designated Approving Authority. In addition, employees are prohibited from processing SUNSI on home computers unless connected to and working within CITRIX, the NRC Broadband Remote Access System. Employees are prohibited from downloading or storing SUNSI to the hard drive of a home computer when connected to and working within CITRIX. Employees are also prohibited expressly from processing SUNSI on home computers even when an encrypted floppy disk, CD, DVD, or thumb drive is the storage media. Employees who work at home must perform electronic processing of SUNSI on either (1) a home computer within the virtual environment provided by the agency through CITRIX or (2) an NRC-issued laptop with NRC-approved encryption software. top
USE WHILE TRAVELING OR COMMUTING	
May I use the information while on official travel or commuting to or from work?	Yes. Abide by the following requirements: • Use of the information is discouraged while traveling on public transportation. To ensure that the information is not viewed or accessed inadvertently or willfully, the employee must ensure that it cannot be seen by persons not authorized access. Particular care should be taken on a public conveyance or in waiting rooms where others may be sitting and standing in close proximity to where the information is being used. • Individuals should hand carry protected information during travel only if other means for transmitting the information, e.g., mailing ahead, faxing, are not readily available or are operationally unacceptable. If hand carrying is determined to be the best transport method, care must be exercised to ensure that the information is not compromised through loss or inadvertent access. • Information must be kept in the traveler's personal possession to extent possible, and stored, appropriately wrapped, in hotel security facilities if possible. • Information must not be saved/stored on a personally owned computer. Work must be performed on an encrypted laptop computer or other encrypted mobile IT device to preclude unauthorized access if the laptop or device is lost or stolen. • The information should be returned to an NRC authorized storage location at the earliest possible opportunity. top
PHYSICAL COPY TRANSMISSION	
May I transmit paper or electronic media including CD-ROM, disk or tape?	Yes. Abide by the following requirements: **Inside the NRC (including Regions):** Information may be – • Hand-carried. • Sent via NRC's interoffice mail system. • Sent via NRC pouch service between headquarters and the regions. Transmit in a single opaque envelope. • Sent via approved commercial express carriers between headquarters and the regions (time-sensitive material only; use NRC Form 420). Transmit in a single opaque envelope.

Outside the NRC: Information may be transmitted by –

- NRC Messenger/NRC contractor messenger.
- U.S. Postal Service: First Class Mail, Registered Mail, Express Mail, Certified Mail.
- Hand-carried by any individual authorized access to the information. That individual shall retain the information in his or her possession to the maximum extent possible unless they place the document in the custody of another person authorized access.
- Approved commercial express carriers (time-sensitive material only; use NRC Form 420); Transmit in single opaque envelope.
- Other means approved by OIS and the Director, Division of Facilities and Security, ADM.

Incoming to the NRC: Electronic submissions, including CD-ROMs, submitted to the NRC should follow the E-Rule "Guidance for Electronic Submission to the Agency," available on NRC's external Web site at http://www.nrc.gov/site-help/eie.html.

Encryption:

All electronic media (CD-Rom, disk, tape, hard drives, thumb drives, etc.) must be encrypted according to Yellow Announcement no. 157.
(b)(7)(F)

top

ELECTRONIC COPY TRANSMISSION

May I transmit the document electronically by e-mail or fax?

Yes. Abide by the following requirements:

Inside the NRC (including Regions): Information may be e-mailed or faxed.

Outside the NRC: Information may be transmitted by –

- Fax: May use non-secure facilities where it is confirmed that a recipient who is authorized to access the information will be present to receive the transmission.
- Email: Encryption is currently not required by the NRC. A separate policy to address encryption of transmitted data will be issued by the Computer Security Office when it is approved.
- Otherwise, transmit a physical copy in the manner set forth above.

Electronic files must contain appropriate markings.

top

STORAGE

Inside the NRC (Headquarters and Regional Offices): Store openly or in non-locking container within areas where there is supplemental security including electronic access controls (keycard) and/or guards on duty. If management determines additional protection is needed, the information should be stored in key locked file cabinets or equivalent storage containers.

Outside the NRC (Resident Inspector Sites): When supplemental security such as electronic access are either unavailable or guards are not on duty, store in key locked desks or other key locked containers.

On NRC Electronic Systems: May be stored on NRC encrypted computer systems that have a Security Plan and Accreditation Approval under MD 12.5.

For storage requirements of other Federal-, State-, Foreign Government-, and International Agency-Controlled Information use their guidelines (see).

top

DESTRUCTION

Official Record Version: Destroy in accordance with NRC Comprehensive Records Disposition Schedule (NUREG-0910).

Non-Official Record Copies:

- Destroy copies other than the official record version by any means that prevents reconstruction in whole or part, including the following methods:
- Place in Classified and Sensitive Unclassified Waste Disposal Containers.
- Tear into one-half inch pieces or smaller.
- Destroy by burning, pulping, pulverizing, shredding or chemical decomposition.

Electronic Data: Use special approaches to delete sensitive unclassified data from electronic storage media. These approaches, as mentioned in the MD 12.5 Handbook, include –

- Destruction of the physical media.
- Obliteration or wiping of the sensitive data through use of an approved software product such as BCWIPE or SDELETE.
- Erasure of all data through degaussing.

top

DECONTROL AUTHORITY

Originating office or office primarily responsible for the information.

top

Page content maintained by: Donna Sealing at SUNSI.Resource@nrc.gov
Last updated: April 27, 2010 1:51 PM

UNITED STATES
NUCLEAR REGULATORY COMMISSION

Announcement No. 077

Date: October 26, 2005

To: **All NRC Employees**

SUBJECT: **POLICY REVISION: NRC POLICY AND PROCEDURES FOR HANDLING, MARKING, AND PROTECTING SENSITIVE UNCLASSIFIED NON SAFEGUARDS INFORMATION (SUNSI)**

In January 2005, I asked the Director, Office of Information Services (OIS), to establish a working group to implement the recommendations of the Sensitive Unclassified Non-Safeguards Information (SUNSI) task force. The group provided its recommended implementation plan and policy to me on September 14, 2005, and I issued that policy for immediate implementation in a memorandum to office directors and regional administrators dated October 26, 2005. This announcement communicates the new policy and procedures.

The new "NRC Policy For Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information" is available at (b)(7)(F), establishes NRC SUNSI policy, and establishes handling requirements in 14 different areas for each of seven SUNSI groups. It is important to note that the SUNSI policy and the handling requirements do not apply to Classified and Safeguards Information.

This announcement supersedes NRC Announcement 2003-079, Interim Guidance for Official Use Only (OUO) Information, issued on September 26, 2003, and contains several other significant changes:

- The current "Official Use Only" cover sheet and the yellow "Proprietary" cover sheet are discontinued.
- Cover sheets are required only for "allegation information" and "investigation information."
- Cover sheets shall not be used for other SUNSI groups.
- Portion marking is not required.

Numerous other changes are reflected in the Communication Plan at (b)(7)(F) that was attached to the memorandum to the office directors.

Additionally, over the next four months, SUNSI awareness training sessions will be held in the auditorium and the schedule will be communicated. Staff should take advantage of these training sessions to become familiar with the new policy. Further training will be incorporated into the Computer Based Learning (CBT) class on Information Computer Security in the spring of 2006.

The new policy and procedures supersede requirements now contained in MD 12.6, "NRC Sensitive Unclassified Information Security Program," and NUREG/BR-0268, "Sensitive Unclassified Information," that apply to non-safeguards sensitive unclassified information. OIS will incorporate these provisions in the next revision of Management Directive (MD) 12.6. Other guidance will also be available at the SUNSI Web site to assist the staff in implementing the requirements.

If you have any questions regarding this policy and procedures, contact Myron Kemerer, OIS, at 301-415-8735 or e-mail mlk2@nrc.gov.

/RA/

(b)(7)(F)

Luis A. Reyes
Executive Director of Operations

NRC Yellow Announcements Index

POLICY ISSUE
(Notation Vote)

October 19, 2004 SECY-04-0191

FOR: The Commissioners

FROM: Luis A. Reyes
Executive Director for Operations /RA/

SUBJECT: WITHHOLDING SENSITIVE UNCLASSIFIED INFORMATION CONCERNING NUCLEAR POWER REACTORS FROM PUBLIC DISCLOSURE

PURPOSE:

To obtain Commission approval of guidance to be issued to the Nuclear Regulatory Commission (NRC) staff, power reactor licensees, and other agency stakeholders for withholding sensitive unclassified (nonsafeguards) information from public disclosure.

SUMMARY:

In a staff requirements memorandum dated May 7, 2004, the Commission directed the NRC staff to develop guidance to ensure information that could reasonably be expected to be useful to potential adversaries is withheld from public disclosure. In determining whether information should be withheld or released, the NRC staff must attempt to appropriately balance our desire to maintain the openness of NRC's regulatory processes with the need to protect the public from possible terrorist threats. This paper provides for Commission review and approval the NRC staff's proposed approach for determining the appropriate handling of information and more specific guidance for withholding or releasing information about nuclear power reactors (Attachment 1).

CONTACTS: William D. Reckley, NRR/IRT
301-415-1323

Margie Kotzalas, NRR/IRT
301-415-2737

BACKGROUND:

In the aftermath of September 11, 2001, the NRC has been challenged, as have other government and private institutions, to assess and revise controls on withholding from public disclosure information that might be useful to terrorists. The NRC policies and criteria for withholding information currently available to external stakeholders are described in COMSECY-02-0015, "Withholding Sensitive Homeland Security Information From the Public," dated April 4, 2002, and the associated SRM dated May 28, 2002. COMSECY-02-0015 provided criteria for withholding information from public disclosure and a general standard that information should be withheld when its release would provide a clear and significant benefit to a terrorist in a potential attack. In COMSECY-03-0036, "Update on the Withholding From Public Disclosure of Sensitive, Unclassified Information Related to Power Reactors," dated July 17, 2003, the staff proposed clarifications to the guidance in COMSECY-02-0015 and provided draft guidance on protecting sensitive information for the NRC staff and nuclear power reactor licensees.

The SRM dated May 7, 2004, instructed the staff to revise the basic standard for withholding information from the public to cover information that "could reasonably be expected to be useful" to terrorists in planning or executing an attack. The SRM also directed the staff to ensure that NRC guidance is consistent with regulations and guidance promulgated by the Department of Homeland Security (DHS) and addresses issues identified during the use of the existing criteria and guidance for withholding sensitive information. The Commission directed the staff to announce and explain the revised guidance to NRC personnel, licensees, and other agency stakeholders.

DISCUSSION:

The NRC has traditionally provided the public with a significant amount of information about the facilities and materials for which the NRC has regulatory responsibilities. This policy has been and remains a cornerstone of the NRC's regulatory philosophy. The Atomic Energy Act, subsequent legislation, and various NRC regulations, have given the public the right to participate in the licensing and oversight process for nuclear power reactors and other NRC licensees. To participate in a meaningful way, the public must have access to information about the design and operation of regulated facilities or materials. However, the NRC and other government agencies have always withheld some information from public disclosure for reasons of security, personal privacy, and commercial or trade secrets. In light of increased terrorist activity worldwide, the NRC has reexamined its traditional practice of releasing almost all documents to the public. The NRC will continue to work with DHS and other agencies to develop and implement any new guidance or requirements that may impact our strategy to communicate openly with the public.

Per the Commission's direction, the goal of establishing guidance for the NRC staff and licensees is to withhold information that could reasonably be expected to be useful to potential adversaries while minimizing the adverse effects on the NRC goals of openness and effectiveness. The attempt to weigh each of the agency's key goals and reach a balanced decision, inevitably introduces a certain amount of subjective judgment with respect to most

information about the design and operation of nuclear power plants. However, the NRC staff's experience is that you must consider the various competing factors to develop a logical and consistent decision regarding the handling of information. Guidance for reaching a balanced decision was provided in COMSECY-02-0015 and has proven useful to the staff in assessing the appropriate handling of specific documents. Unlike safeguards information (SGI) and security-related information within the reactor oversight process, which deal primarily with security programs, most information on nuclear reactors is developed and maintained to support areas such as engineering, operations, and licensing. The potential usefulness of this information to an adversary is in showing how a facility is constructed or operated, not how it is protected in terms of security. The difficulty in withholding such information is that much of it relates to how a facility was licensed and how it is maintained. The information provides the means for the NRC and public to assess the safety of the facility in areas other than security. Stringent restrictions on information related to plant design and operation (i.e., not directly related to security) could have a negative impact on safety if the controls result in less sharing of information among the appropriate licensee personnel. Therefore, the staff has developed the following general approach, as well as more specific criteria, for controlling information on nuclear power reactors.

The staff is limiting this guidance to nuclear power reactors and will prepare separate consistent guidance for other types of licensed activities.[1] The staff believes this is appropriate because a realistic evaluation of the appropriate controls on information needs to consider the threats, the risks of potential attacks, the security programs in place, and other factors that vary widely among the different types of licensees. For the most part, the staff used this approach in interpreting and implementing the guidance in COMSECY-02-0015. For nuclear reactors, most information on security that is addressed by the criteria in COMSECY-02-015 has been and continues to be controlled as SGI. In addition to the information on security programs, the staff has withheld information regarding some aspects of plant design (e.g., detailed layout drawings of sites or buildings), risk insights comparable to individual plant examination (IPE) documents in terms of identifying critical combinations of equipment, and current plant configurations. In COMSECY-03-0036, the staff proposed to revise the criteria and usually release documents providing risk insights for nuclear power plant designs and operations because such information is already available in the public domain and the withholding of such information is increasingly awkward as the agency moves to incorporate such risk insights into its routine decisionmaking. The SRM dated May 7, 2004, directed the staff to revise the clarifications proposed in COMSECY-03-0036 and the guidance established in COMSECY-02-0015 and the associated SRM.

---

[1] The staff outlined in SECY-04-0155, "Request From Department of Energy Office of Naval Reactors to Designate Information Related to Nuclear Fuel Services, Inc. And BWX Technologies, Inc., As 'Official Use Only'," dated August 24, 2004, the steps taken and guidance provided to remove information from public access related to Category I fuel cycle facilities.

In determining what information "could reasonably be expected to be useful to potential adversaries," one needs to assess the relevance of the specific information to an adversary's ability to plan or execute an attack or other malevolent act and the ability of a licensee or government agency to respond to such an attack. It is important to develop a logical assessment approach to ensure consistency, to ensure that appropriate information is withheld from public disclosure, and to minimize adverse effects on the agency's openness and effectiveness. It is also important to maintain an appropriate and realistic view about the added security assurance provided by the control of non-SGI information. The withholding of certain design or operational information may introduce a hurdle for potential adversaries during their planning of a malevolent act. The effectiveness of the hurdle, however, depends on the assumed level of sophistication, education, and knowledge of the adversaries. In some cases, it may be more appropriate to assess and, if necessary, revise a security program in recognition that the subject information is in the public domain.

The discussion below is not intended to illustrate a detailed threat or vulnerability assessment since decisions regarding the release or withholding of most information are expected to be made at the staff level within each program office. The following factors provide a general framework that may be used to develop more specific guidance for different types of facilities or materials.

- The threat

  The control of information as part of an overall program to safeguard against the intentional release or diversion of radioactive materials needs to consider those threats for which the withholding of information might be helpful. The assessment is not limited to or even related to the design basis threat (DBT) but instead needs to consider the range of possible malevolent acts against a nuclear power reactor or other licensed activity. The assessments and evaluations are, at this point, based largely on staff judgments unless more detailed simulations, vulnerability assessments, or other guidance are available.

- The consequences

  For each of the possible threats, there is a possible consequence in terms of harm to the public. The consequences of an event involving a nuclear reactor include the possible release of radioactive materials that might adversely affect public health and safety. In the worst case, an attack on a nuclear reactor could cause plant transients and losses of mitigating systems, leading to core damage and a major release of fission products. The consequences for other threats involve lesser releases (e.g., from waste systems) or possibly no releases of radioactive materials. The possible consequences associated with a particular licensed activity are usually reflected in the licensing processes and regulatory controls placed on those activities. The decision to withhold or release information needs to consider the possible consequences of events such that our controls on information correlate to the potential harm (i.e., information would not be treated as sensitive unless it relates to the potential release or diversion of radioactive materials posing a threat to public health and safety).

- The relationship of design/operating limits to security programs

  Information related to security programs at nuclear reactors is generally designated as SGI and is protected in a manner similar to classified confidential information. For nuclear reactors, the security program is quite extensive and is established to protect the plant, including the engineering barriers designed to prevent the release of radioactive materials, from an attack by potential adversaries. Information on the engineering barriers themselves has largely been part of the public record. For other NRC-licensed activities or nonnuclear critical infrastructure, security programs may not be as extensive and the engineering barriers may also serve as the primary security feature. In such cases, protection of engineering information may be more important from the standpoint of security (after factoring in the other factors such as possible threats and consequences).

- Availability of information from other sources

  In assessing the control of information, it is important to assess the availability of the information or similar information from sources outside the control of the NRC or its licensees. If the information is available from open source literature such as text books, Web sites, or other sources, an NRC decision to withhold the information may decrease the openness of our regulatory programs without obstructing an adversary.

- Subsequent controls on the information

  In deciding to withhold information coming to or issued by the NRC, we need to consider how the information will be controlled by other parties with access to it. For example, a situation could negatively affect our goals regarding effectiveness or openness if we strive to withhold information and the information is then released by a licensee or other government agency. A consistent treatment of information may evolve as DHS continues to develop requirements or guidance for controlling information shared among licensees and Federal, State, and local governments when the information is designated "sensitive homeland security information."

  This assessment will also address how the information and its controls are incorporated into other licensee and regulatory processes. Any concerns regarding conflicting determinations (e.g., a finding that information should be withheld due to an assessment of its possible usefulness to an adversary and a regulatory need to make the information public) should be reported to agency management for resolution.

The above general criteria are expanded upon and applied to the routine (nonsecurity) documents received and generated by the NRC and power reactor licensees to develop the specific guidelines and examples provided in Attachment 1.

The staff has evaluated the information categories developed by other Federal agencies and will include a discussion of the designations with possible implications for nuclear reactors in the guidance being prepared for the NRC staff and licensees. The NRC staff will, whenever possible, maintain practices consistent with other government agencies that are controlling

information related to facilities located near nuclear power reactors. The major designations of information with a potential to affect nuclear reactors are discussed in Attachment 2. A short discussion of selected designations is provided below:

- Protected Critical Infrastructure Information (PCII): PCII is voluntarily provided to DHS, is not customarily in the public domain, and is related to the security of critical infrastructure or protected systems. The NRC staff does not expect that the NRC or nuclear power reactor licensees will need to deal very often with information designated as PCII because nearly all information related to security is addressed by NRC regulations and oversight programs.

- Critical Energy Infrastructure Information (CEII): CEII is a designation defined in the regulations of the Federal Energy Regulatory Commission (FERC) at Title 18 CFR Parts 375 and 388 for information related to energy-related infrastructure. FERC provided additional guidance related to CEII in its rulemaking documents. There is some overlap in the information provided to the NRC by power reactor licensees regarding nearby energy-related facilities (e.g., hydroelectric dams, electric transmission systems) and the information routinely treated as CEII by FERC. Likewise information related to the location of pipelines may warrant review and withholding per guidance from the Department of Transportation. Most of the information regarding electric transmission systems provided to FERC (through its periodic Form 715) is designated CEII. The NRC staff believes we will need to make public some information on electric transmission systems supporting nuclear power plants since the information is integral to major licensing decisions and related environmental findings.

- Homeland Security Information (HSI): The term HSI was introduced in the Homeland Security Act of 2002, 6 USC 482, as part of the effort to ensure that information related to possible terrorist activities would be shared between the appropriate Federal, State, and local governments.

- Sensitive Homeland Security Information (SHSI): The term SHSI has been proposed to address the HSI that must be shared between Federal, State, and local agencies while being withheld from public disclosure. DHS continues to work on requirements and guidance to fully develop the SHSI designation. Given its relationship to HSI and the sharing of information with appropriate agencies, the staff believes that SHSI related to nuclear power plants will most likely involve some information on potential threats and the coordination of responses to a terrorist attack. If information is being shared only between a licensee and the NRC, the staff would more likely use the provisions of 10 CFR 2.390 to withhold the information from public disclosure.

NRC regulations at 10 CFR 2.390 provide a mechanism to withhold from public disclosure information related to the physical protection of nuclear power plants that does not meet the existing criteria for designation as SGI. This type of information was recognized before September 11, 2001, and, when submitted to the NRC by a licensee, was withheld from public disclosure and handled similarly to commercial or financial information as directed by the regulation. The NRC has expanded the application of this regulation to address sensitive

unclassified (non-SGI) information previously made public but now withheld if the information could be useful to a potential adversary (e.g., detailed layout drawings and selected inspection reports). The staff expects that the volume of material withheld from public disclosure according to 10 CFR 2.390 will continue to increase as the process is explained to licensees and the NRC staff. The staff will continue the historical practice of waiving the requirement for an affidavit from the licensee when a request for withholding information (similar to commercial or financial information) is made in accordance with 10 CFR 2.390 because the information concerns a facility's physical protection.

The SRM dated May 7, 2004, directed the staff to consider the experiences and lessons learned since the review activities were initiated following September 11, 2001. The biggest issue related to the withholding of information on power reactors concerns the guidance in COMSECY-02-0015 to withhold risk insights similar to the risk insights provided in documents such as individual plant examinations (IPEs). If the desire is to keep from adversaries the list of important mitigating systems, the staff believes the effort would have little or no benefit because such information is available in open source literature. It may be possible, however, to at least impede efforts by adversaries to obtain information on the plant-specific location of many important components. As a point of clarification, the staff has not withheld and does not expect to withhold information regarding risk importance measures for specific plant systems since these numerical values could not reasonably be expected to be useful to an adversary. A stronger argument could be made for withholding documents that identify specific combinations of systems whose loss, when combined with an identified initiating event, results in core damage. However, this information is available in the public domain, and the staff does not foresee withholding such information for power reactors unless it is related to security activities (e.g., vulnerability assessments). Another issue related to the withholding of information on power reactors concerns both ongoing and past adjudications, including the hearing files, testimony, documents which must be provided in discovery, and documents supporting staff conclusions and licensing actions. Because the public has the right to participate in varying ways in the licensing and other regulatory processes associated with NRC-licensed facilities, the withholding of certain information in staff documents related to those processes may need to be modified on a case-by-case basis. For example, certain information may not be able to be withheld at all under applicable statutory and case law, while other information may have to be provided to parties to proceedings under protective orders. The staff will consult with OGC in such circumstances.

The staff plans to conduct public meetings and issue guidance to the staff, licensees, and stakeholders as soon as practical after finalizing the agency's position on the designation of information as sensitive unclassified (non-SGI) information. The meetings and related interactions will also enable the staff to discuss with stakeholders the potential need for changes in licensees' document control practices to protect sensitive unclassified (non-SGI) information.

RECOMMENDATIONS:

We recommend the Commission approve (1) the general framework presented in this paper for making decisions on withholding information because its release could reasonably be expected to be useful to an adversary and (2) the specific guidance provided in Attachment 1 for making such determinations for information related to nuclear power reactors.

COORDINATION:

The Office of the General Counsel has reviewed this paper and has no legal objections to its content.

/RA/

Luis A. Reyes
Executive Director
for Operations

Attachments: 1. Handling of Sensitive Unclassified (Nonsafeguards) Information on Nuclear Power Reactors That Could Reasonably Be Expected to Be Useful to a Potential Adversary
2. Terminology and Other Government Designations

Handling of Sensitive Unclassified (Nonsafeguards) Information on Nuclear Power Reactors That Could Reasonably Be Expected to Be Useful to a Potential Adversary

Safeguards information (SGI) is information not otherwise classified as national security information or restricted data which specifically identifies a licensee's or applicant's detailed, (1) security measures for the physical protection of special nuclear material or (2) security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization facilities. However, there may be information that could reasonably be expected to be useful to a potential adversary that does not meet the requirements established for designating the information as SGI. This information will be treated as sensitive unclassified (non-SGI) information in accordance with established agency procedures and regulations. Information obtained from or provided to licensees and determined to be sensitive unclassified (non-SGI) information should be treated similar to commercial or financial information and withheld from public disclosure under 10 CFR 2.390. Information shared with other government agencies and licensees may be treated in a similar fashion unless addressed by other handling requirements (e.g., sensitive homeland security information).

In determining what information "could reasonably be expected to be useful to potential adversaries," one needs to assess the relevance of the specific information to an adversary's ability to plan or execute an attack or other malevolent act and the ability of a licensee or government agency to respond to such an attack. The discussion below is not intended to exemplify detailed threat or vulnerability assessments since decisions regarding the release or withholding of most information are expected to be made at the staff level within each program office. It is presented here to provide a thought process that has generally been consistent with the staff's intuitive evaluation of information.

The control of information needs to consider the following factors:

- The threat

  The control of information as part of an overall program to safeguard against the intentional release of radioactive materials needs to consider those threats for which the withholding of information might be helpful. The assessment is not limited to or even related to the design basis threat (DBT) but should consider the entire range of possible malevolent acts against a nuclear power reactor or other licensed activity. The assessments and evaluations are, at this point, based largely on staff judgments unless more detailed simulations or vulnerability assessments are available. The wide range of possible attacks against a nuclear power plant means that few issues will be decided based on the absence of a credible threat. For example, detailed layout drawings of the facility are to be withheld to ensure they do not assist adversaries in planning an attack on critical plant systems even though a security program is in place to thwart such an attack. The primary protection against an attack on a nuclear power plant is the security program. Information related to the security program that is not otherwise designated as SGI (e.g., information on training, inspection reports, performance assessments) may provide insights into the program and is likely to be withheld in accordance with 10 CFR 2.390.

- The consequences

  For each of the possible threats, there is a possible consequence in terms of harm to the public. The consequences of events involving NRC licensees, including nuclear reactors, include the possible release of radioactive materials that might adversely affect public health and safety. In the worst case, an attack on a nuclear reactor could cause plant transients and losses of mitigating systems, leading to core damage and a major release of fission products. The consequences for other threats could involve lesser releases (e.g., from waste systems) or possibly no releases of radioactive materials. The possible consequences associated with a particular licensed activity is usually reflected in the licensing processes and regulatory controls placed on those activities. The decision to withhold or release information needs to consider the possible consequences of events such that our controls on information correlate to the potential harm (i.e., information would not be treated as sensitive unless it relates to the potential release or diversion of radioactive materials posing a threat to public health and safety). Information related to events that are analyzed and result in doses below established regulatory thresholds (including many design basis accidents) may be released since the consequences have been determined to result in minimal risk to the public health and safety. The staff should consider the possible combinations of events and potential losses of mitigating systems that might result from a terrorist attack before concluding too quickly that the consequences of a threat are adequately addressed by an existing licensing-basis type analysis.

- The relationship of design/operating limits to security programs

  Information related to security programs at nuclear reactors is generally designated SGI and is protected in a manner similar to classified confidential information. For nuclear reactors, the security program is quite extensive and is established to prevent the loss of the engineering barriers designed to prevent the release of radioactive materials. Information regarding the engineering barriers themselves has been part of the public record. The design information may be withheld when it is used in the context of a security-related vulnerability assessment. For example, the traditional analysis of a structure against design basis winds will be released but an analysis related to structural failures from an explosive charge will be withheld.

- The availability of information from other sources

  In assessing the control of information, it is important to assess the availability of the information or similar information from sources outside the control of the NRC or its licensees. If the information is available from open source literature such as text books, Web sites, or other sources, an NRC decision to withhold the information may decrease the openness of our regulatory programs without obstructing an adversary. For example:

  - Information on the geospatial coordinates for facilities is released since this information is readily available in the public realm

  - Information on evacuation routes is released since it is routinely provided to the public for emergency planning purposes

- Information clearly visible from locations accessible to the public near the site is generally released. This includes general (low-resolution) layout drawings of the site and adjacent areas, including drawings showing the plant connections to the electric transmission system.

- Information related to the general workings of a nuclear power plant such as the descriptions usually provided in licensing documents (e.g., updated final safety analysis reports, license renewal applications) are released since similar information (at the level useful to a potential adversary) is available in open source literature such as text books and Internet sites. This level of information includes listings and general descriptions of safety-related and important-to-safety systems (including nonsecurity-related probabilistic risk assessments such as those included in accident sequence precursor analyses, risk-informed changes to technical specifications, and significance determination process notebooks). Information regarding such systems will be withheld in a context such as a vulnerability assessment (e.g., how a system might be affected by attacks or other malevolent acts).

- The subsequent controls on the information

In deciding to withhold information coming to or issued by the NRC, we need to consider how the information will be controlled by other parties with access to it. For example, we may negatively affect our goals regarding effectiveness or openness if we strive to withhold information and the information is then released by a licensee or other government agency. DHS may develop requirements or guidance for controlling information shared between licensees and Federal, State, and local governments when the information is designated "sensitive homeland security information."

This assessment will also address how the information and its controls are incorporated into other licensee and regulatory processes. For example, COMSECY-03-0036 discussed the removal of some specific information from final safety analysis reports (FSARs) to address potential security concerns and the subsequent restoration of the FSARs to the public domain without the need to develop public/nonpublic versions. The proposed handling of FSARs described in COMSECY-03-0036 was also intended to minimize potential adverse effects on regulatory programs such as the evaluations required by 10 CFR 50.59, "Changes, tests, and experiments." Any concerns regarding conflicting determinations (e.g., a finding that information should be withheld due to an assessment of its possible usefulness to an adversary and a regulatory need to make the information public) should be reported to agency management for resolution.

- The requirements and guidance established by other government agencies

  In deciding on the appropriate handling of information received from or provided to licensees, the staff should consider whether rules or guidance from other Federal agencies are in play. If the information is received from another agency and is identified by that agency as sensitive unclassified information, the staff should honor the designation and handle the information accordingly. Most information addressed by other federal agencies and of concern to the NRC staff or reactor licensees relates to infrastructure located near the nuclear power plant. Examples are the designation critical energy infrastructure information (CEII) for information related to hydroelectric dams regulated by the Federal Energy Regulatory Commission (FERC) and the withholding of maps showing pipelines under the jurisdiction of the Department of Transportation. The staff should make every effort to follow the guidance of other agencies in the review and designation of information related to facilities or activities for which another agency has the lead authority. Most of the Information on electric transmission systems provided to FERC (through its periodic Form 715) is designated CEII. Some documents provided to the NRC (e.g., updated final safety analysis reports and environmental reports related to license renewal applications) include information on electric transmission lines associated with nuclear power reactors. The information usually provided to the NRC is a subset of the information reported to FERC and relates only to power lines easily visible from the site environs. The NRC will need to make public some information on electric transmission systems supporting nuclear power plants since the information is integral to major licensing decisions and related environmental findings.

The staff has applied the above guidance to information routinely exchanged between licensees and the NRC to help the staff and licensees evaluate and control documents. The example subjects addressed in the following table include the technical areas identified in Regulatory Guide 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants," as well as several other subjects addressed in routine correspondence associated with nonsecurity-related activities for nuclear power reactors. Information presented in the context of vulnerability assessments or other security-related matters will usually be withheld from public disclosure. These or similar examples will be included in guidance documents and will be routinely updated for use by the staff and licensees.

Control of Information by Subject Matter	
Subject	**Discussion and/or typical controls**
General Description of Plant	Decisions regarding the control of information (usually drawings) that describe plant sites and buildings are dependent on the level of detail. Information clearly visible from locations accessible to the public near the site is generally released. This includes general (low-resolution) layout drawings of the site and adjacent areas. Drawings showing details such as the specific locations of equipment within buildings, doorways, stairways, etc. are to be withheld under 10 CFR 2.390.

Subject	Discussion and/or typical controls
Site Characteristics:	
Geography and demography	Uncontrolled
Nearby Industrial, transportation, and military facilities	Guidance related to the control of information related to non-nuclear facilities located near nuclear power plants may be available from other federal agencies (e.g., DHS, FERC, EPA, DOT). The staff should make every effort to follow the guidance of other agencies in the review and designation of information related to facilities or activities for which another agency has the lead authority. Specific examples include pipeline data (usually withheld per DOT) and chemical facilities (some data withheld per EPA). In addition to the guidance from other agencies, the staff will also withhold information related to nearby industrial facilities if the information might reasonably be helpful to those planning an attack on a nuclear power plant.
Meteorology	Uncontrolled
Hydrologic Engineering	Uncontrolled with the exception of information regarding the design of nearby dams. Information on dams may be designated critical energy infrastructure information by FERC.
Geology, seismology, and geotechnical engineering	Uncontrolled
Design of Structures, Components, Equipment, and Systems	Information regarding the design of structures provided to the NRC typically consists of analyses to show that the design feature will withstand the combinations of forces associated with design basis events and natural hazards. The analyses do not typically provide realistic information on the failure of structural features and are not considered sensitive. Information related to actual structural failures that could be useful to terrorists will be withheld.
Reactor (Nuclear, Thermal-hydraulic designs, Materials)	Uncontrolled
Reactor Coolant System	Uncontrolled

Subject	Discussion and/or typical controls
Engineered Safety Features	Information provided to the NRC on engineered safety features usually relates to their design, maintenance, or operation during routine activities or design basis transients (i.e., nonsecurity related events) and is not treated as sensitive. Detailed layout drawings showing the actual location of equipment is withheld under 10 CFR 2.390. Discussions of safety features or mitigation strategies within vulnerability assessments will also be withheld from public disclosure.
Instrumentation and Controls	Uncontrolled
Electric Power	Information provided to the NRC on offsite and onsite electric power systems typically relate to their design, maintenance, or operation during routine activities or design basis transients (i.e., nonsecurity related events) and is not treated as sensitive. It is necessary for the NRC to make public some information on electric transmission systems supporting nuclear power plants since the information is integral to major licensing decisions and related environmental findings (e.g., information usually provided with license renewal applications). Information on the transmission grid beyond that needed for NRC regulatory decisions is likely to be withheld in accordance with the FERC guidance on critical energy infrastructure information.
Auxiliary Systems (Fuel storage, ultimate heat sink)	Uncontrolled- This includes general (low-resolution) layout drawings of the site and descriptions and drawings such as the arrangement of spent fuel within spent fuel pools. Drawings showing details such as the specific location of equipment, doorways, stairways, etc. are to be withheld under 10 CFR 2.390.
Steam and Power Conversion	Uncontrolled
Radioactive Waste Management	Uncontrolled - This includes general (low-resolution) layout drawings of the site. Drawings showing details such as the specific location of equipment, doorways, stairways, etc. are to be withheld under 10 CFR 2.390.
Radiation Protection	Uncontrolled - This includes general (low-resolution) layout drawings of the site and adjacent areas. Drawings showing details such as the specific location of equipment, doorways, stairways, etc. are to be withheld under 10 CFR 2.390.
Conduct of Operations	Uncontrolled (excluding security)

Subject	Discussion and/or typical controls
Test Program (Initial and Inservice Inspections and Testing)	Uncontrolled
Accident Analysis	Uncontrolled - Accident analyses typically included in licensing-related correspondence involve conservative models to demonstrate a plant's ability to respond to design basis transients (i.e., nonsecurity related events), and is not treated as sensitive.
Technical Specifications (including Bases)	Uncontrolled
Quality Assurance	Uncontrolled
Fire Protection	Incoming documents are initially profiled as nonpublic - staff will review for release upon request. Most information related to fire protection will not need to be designated as sensitive. Drawings showing details such as the specific location of equipment, doorways, stairways, etc. are to be withheld under 10 CFR 2.390.
Emergency Planning	Incoming documents are initially profiled as nonpublic - staff will review for release upon request. Most information related to emergency planning will not need to be designated as sensitive. Special attention is needed to determine if information relates to the response by a licensee or government agency to a terrorist attack. Note that some State and local governments consider parts of their emergency plans to be sensitive.
Security	Information related to security programs at nuclear reactors is generally designated as SGI and is protected in a manner similar to classified confidential information. Security-related information within the inspection program and reactor oversight process is withheld from public disclosure under 10 CFR 2.390.
Risk-Informed Decisionmaking (e.g., documents related to risk-informed licensing actions, accident sequence precursor (ASP) analyses, significance determination process (SDP) notebooks, design certifications)	Uncontrolled - exceptions include information related to security activities (e.g., vulnerability assessments) and information related to uncorrected configurations or conditions that could be useful to an adversary. Special attention should be applied to this area and information should be withheld if it describes a vulnerability or plant-specific weakness that is more helpful to an adversary than are the insights provided in open source literature. Detailed computer models have been and will continue to be withheld from public disclosure.

Subject	Discussion and/or typical controls
Inspections & Performance Assessment	Uncontrolled - exceptions include information on security-related inspections or performance assessments and information related to uncorrected vulnerabilities that could be useful to an adversary.
Current Plant Configurations	Information on current plant configurations or conditions that could be useful to an adversary (e.g., important safety equipment out of service) is withheld from public disclosure (usually by simply timing its release) until such time as the information no longer reflects current plant conditions.

Terminology and Other Government Designations

Several discussions or definitions related to this issue are provided below:

- **Section 147, "Safeguards Information," of the Atomic Energy Act, as amended, 42 USC §2167, states:**

  a. In addition to any other authority or requirement regarding protection from disclosure of information, and subject to subsection (b)(3) of section 552 of title 5, the Commission shall prescribe such regulations, after notice and opportunity for public comment, or issue such orders, as necessary to prohibit the unauthorized disclosure of safeguards information which specifically identifies a licensee's or applicant's detailed -

  (1) control and accounting procedures or security measures (including security plans, procedures, and equipment) for the physical protection of special nuclear material, by whomever possessed, whether in transit or at fixed sites, in quantities determined by the Commission to be significant to the public health and safety or the common defense and security;

  (2) security measures (including security plans, procedures, and equipment) for the physical protection of source material or byproduct material, by whomever possessed, whether in transit or at fixed sites, in quantities determined by the Commission to be significant to the public health and safety or the common defense and security; or

  (3) security measures (including security plans, procedures, and equipment) for the physical protection of and the location of certain plant equipment vital to the safety of production or utilization facilities involving nuclear materials covered by paragraphs (1) and (2) if the unauthorized disclosure of such information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of such material or such facility. The Commission shall exercise the authority of this subsection -

  (A) so as to apply the minimum restrictions needed to protect the health and safety of the public or the common defense and security, and

  (B) upon a determination that the unauthorized disclosure of such information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of such material or such facility.

- **§ 73.2 Title 10 of Code Federal Regulations**

Safeguards Information means information not otherwise classified as National Security Information or Restricted Data which specifically identifies a licensee's or applicant's detailed, (1) security measures for the physical protection of special nuclear material, or (2) security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization facilities.

- **§ 73.21 Title 10 of Code Federal Regulations**

(b) *Information to be protected.* The specific types of information, documents, and reports that shall be protected are as follows:
(1) *Physical protection at fixed sites.* Information not otherwise classified as Restricted Data or National Security Information relating to the protection of facilities that possess formula quantities of strategic special nuclear material, and power reactors. Specifically:
(i) The composite physical security plan for the nuclear facility or site.
(ii) Site specific drawings, diagrams, sketches, or maps that substantially represent the final design features of the physical protection system.
(iii) Details of alarm system layouts showing location of intrusion detection devices, alarm assessment equipment, alarm system wiring, emergency power sources, and duress alarms.
(iv) Written physical security orders and procedures for members of the security organization, duress codes, and patrol schedules.
(v) Details of the on-site and off-site communications systems that are used for security purposes.
(vi) Lock combinations and mechanical key design.
(vii) Documents and other matter that contain lists or locations of certain safety-related equipment explicitly identified in the documents as vital for purposes of physical protection, as contained in physical security plans, safeguards contingency plans, or plant specific safeguards analyses for production or utilization facilities.
(viii) The composite safeguards contingency plan for the facility or site.
(ix) Those portions of the facility guard qualification and training plan which disclose features of the physical security system or response procedures.
(x) Response plans to specific threats detailing size, disposition, response times, and armament of responding forces.
(xi) Size, armament, and disposition of on-site reserve forces.
(xii) Size, identity, armament, and arrival times of off-site forces committed to respond to safeguards emergencies.
(xiii) Information required by the Commission pursuant to 10 CFR 73.55 (c) (8) and (9).

(2) *Physical protection in transit.* Information not otherwise classified as Restricted Data or National Security Information relative to the protection of shipments of formula quantities of strategic special nuclear material and spent fuel. Specifically:
(i) The composite transportation physical security plan.
(ii) Schedules and itineraries for specific shipments. (Routes and quantities for shipments of spent fuel are not withheld from public disclosure. Schedules for spent fuel shipments may be released 10 days after the last shipment of a current series.)
(iii) Details of vehicle immobilization features, intrusion alarm devices, and communication systems.
(iv) Arrangements with and capabilities of local police response forces, and locations of safe havens.
(v) Details regarding limitations of radio-telephone communications.
(vi) Procedures for response to safeguards emergencies.
(3) *Inspections, audits and evaluations.* Information not otherwise classified as National Security Information or Restricted Data relating to safeguards inspections and reports. Specifically:
(i) Portions of safeguards inspection reports, evaluations, audits, or investigations that contain details of a licensee's or applicant's physical security system or that disclose uncorrected defects, weaknesses, or vulnerabilities in the system. Information regarding defects, weaknesses or vulnerabilities may be released after corrections have been made. Reports of investigations may be released after the investigation has been completed, unless withheld pursuant to other authorities, e.g., the Freedom of Information Act (5 U.S.C. 552).
(4) *Correspondence.* Portions of correspondence insofar as they contain Safeguards Information specifically defined in paragraphs (b)(1) through (b)(3) of this paragraph.

- **Critical Infrastructure Information is defined in Title 6 CFR Part 29 as:**

Critical Infrastructure Information, or CII means information not customarily in the public domain and related to the security of critical infrastructure or protected systems. CII consists of records and information concerning: (1) Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms the interstate commerce of the United States, or threatens public health or safety; (2) The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation, risk-management planning, or risk audit; or (3) Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

- **Protected CII is defined in Title 6 CFR Part 29 as:**

  Protected Critical Infrastructure Information, or Protected CII means CII (including the identity of the submitting person or entity) that is voluntarily submitted to DHS for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement as described in Sec. 29.5. This information maintains its protected status unless DHS's Protected CII Program Manager or the Protected CII Program Manager's designees render a final decision that the information is not Protected CII.

- **Homeland Security Information is defined in Section 892(f)(1) of the Homeland Security Act of 2002, 6 USC 482, as:**

  any information possessed by Federal, State, or local agency that:
  (A) relates to the threat of terrorist activity;
  (B) relates to the ability to prevent, interdict, or disrupt terrorist activity;
  (C) would improve the identification or investigation of a suspected terrorist or terrorists organization; or
  (D) would improve the response to a terrorist act."

- **Sensitive Homeland Security Information**

  The Department of Homeland Security continues to develop guidance related to sensitive homeland security information (SHSI). The staff will continue to monitor the DHS activities in this area. The definition is expected to be related to the definition of homeland security information provided above. The designation of information as SHSI would be expected to help protect the information from public disclosure while also maintaining the free flow of such information between Federal, State, and Local governments.

- **Critical Energy Infrastructure Information**

  The Federal Energy Regulatory Commission has provided a definition of Critical Energy Infrastructure Information in their regulations at 18 CFR Parts 375 and 388. § 388.113 states :

  (1) Critical energy infrastructure information means information about proposed or existing critical infrastructure that: (i) Relates to the production, generation, transportation, transmission, or distribution of energy; (ii) Could be useful to a person in planning an attack on critical infrastructure; (iii) Is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552; and (iv) Does not simply give the location of the critical infrastructure.

- **Sensitive Security Information (Transportation)**

The Transportation Safety Administration and Department of Transportation have provided the following definition of "sensitive security information" or SSI in their regulations at 49 CFR Part 15. See interim final rule published May 18, 2004 (69 FR 28066).

Sec. 15.5 Sensitive security information.

(a) In general. In accordance with 49 U.S.C. 40119(b)(1), SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which the Secretary of DOT has determined would-- (1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file); (2) Reveal trade secrets or privileged or confidential information obtained from any person; or (3) Be detrimental to transportation safety. (b) Information constituting SSI. Except as otherwise provided in writing by the Secretary of DOT in the interest of public safety or in furtherance of transportation security, the following information, and records containing such information, constitute SSI:

(1) Security programs and contingency plans. Any security program or security contingency plan issued, established, required, received, or approved by DOT or DHS, including-- (i) Any aircraft operator or airport operator security program or security contingency plan under this chapter; (ii) Any vessel, maritime facility, or port area security plan required or directed under Federal law; (iii) Any national or area security plan prepared under 46 U.S.C. 70103; and (iv) Any security incident response plan established under 46 U.S.C. 70104.

(2) Security Directives. Any Security Directive or order-- (i) Issued by TSA under 49 CFR 1542.303, 1544.305, or other authority; (ii) Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR part 6, or 33 U.S.C. 1221 et seq. related to maritime security; or (iii) Any comments, instructions, and implementing guidance pertaining thereto.

(3) Information Circulars. Any notice issued by DHS or DOT regarding a threat to aviation or maritime transportation, including any-- (i) Information Circular issued by TSA under 49 CFR 1542.303 or 1544.305, or other authority; and (ii) Navigation or Vessel Inspection Circular issued by the Coast Guard related to maritime security.

(4) Performance specifications. Any performance specification and any description of a test object or test procedure, for-- (i) Any device used by the Federal government or any other person pursuant to any aviation or maritime transportation security requirements of Federal law for the detection of any weapon, explosive, incendiary, or destructive device or substance; and (ii) Any communications equipment used by the Federal government or any other person in carrying out or complying with any aviation or maritime transportation security requirements of Federal law.

(5) Vulnerability assessments. Any vulnerability assessment directed, created, held, funded, or approved by the DOT, DHS, or that will be provided to DOT or DHS in support of a Federal security program.

(6) Security inspection or investigative information. (i) Details of any security inspection or investigation of an alleged violation of aviation or maritime transportation security requirements of Federal law that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or audit. (ii) In the case of inspections or investigations performed by TSA, this includes the following information as to events that occurred within 12 months of the date of release of the information: the name of the airport where a violation occurred, the airport identifier in the case number, a description of the violation, the regulation allegedly violated, and the identity of any aircraft operator in connection with specific locations or specific security procedures. Such information will be released after the relevant 12-month period, except that TSA will not release the specific gate or other location on an airport where an event occurred, regardless of the amount of time that has passed since its occurrence. During the period within 12 months of the date of release of the information, TSA may release summaries of an aircraft operator's, but not an airport operator's, total security violations in a specified time range without identifying specific violations or locations. Summaries may include total enforcement actions, total proposed civil penalty amounts, number of cases opened, number of cases referred to TSA or FAA counsel for legal enforcement action, and number of cases closed.
(7) Threat information. Any information held by the Federal government concerning threats against transportation or transportation systems and sources and methods used to gather or develop threat information, including threats against cyber infrastructure.
(8) Security measures. Specific details of aviation or maritime transportation security measures, both operational and technical, whether applied directly by the Federal government or another person, including-- (i) Security measures or protocols recommended by the Federal government; (ii) Information concerning the deployments, numbers, and operations of Coast Guard personnel engaged in maritime security duties and Federal Air Marshals, to the extent it is not classified national security information; and (iii) Information concerning the deployments and operations of Federal Flight Deck Officers, and numbers of Federal Flight Deck Officers aggregated by aircraft operator. (9) Security screening information. The following information regarding security screening under aviation or maritime transportation security requirements of Federal law: (i) Any procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo, that is conducted by the Federal government or any other authorized person. (ii) Information and sources of information used by a passenger or property screening program or system, including an automated screening system. (iii) Detailed information about the locations at which particular screening methods or equipment are used, only if determined by TSA to be SSI. (iv) Any security screener test and scores of such tests. (v) Performance or testing data from security equipment or screening systems. [[Page 28080]] (vi) Any electronic image shown on any screening equipment monitor, including threat images and descriptions of threat images for threat image projection systems.
(10) Security training materials. Records created or obtained for the purpose of training persons employed by, contracted with, or acting for the Federal government or another person to carry out any aviation or maritime transportation security measures required or recommended by DHS or DOT.

(11) Identifying information of certain transportation security personnel. (i) Lists of the names or other identifying information that identify persons as-- (A) Having unescorted access to a secure area of an airport or a secure or restricted area of a maritime facility, port area, or vessel or; (B) Holding a position as a security screener employed by or under contract with the Federal government pursuant to aviation or maritime transportation security requirements of Federal law, where such lists are aggregated by airport; (C) Holding a position with the Coast Guard responsible for conducting vulnerability assessments, security boardings, or engaged in operations to enforce maritime security requirements or conduct force protection; (D) Holding a position as a Federal Air Marshal; or (ii) The name or other identifying information that identifies a person as a current, former, or applicant for Federal Flight Deck Officer.
(12) Critical aviation or maritime infrastructure asset information. Any list identifying systems or assets, whether physical or virtual, so vital to the aviation or maritime transportation system that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is-- (i) Prepared by DHS or DOT; or (ii) Prepared by a State or local government agency and submitted by the agency to DHS or DOT.
(13) Systems security information. Any information involving the security of operational or administrative data systems operated by the Federal government that have been identified by the DOT or DHS as critical to aviation or maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems.
(14) Confidential business information. (i) Solicited or unsolicited proposals received by DHS or DOT, and negotiations arising therefrom, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, but only to the extent that the subject matter of the proposal relates to aviation or maritime transportation security measures; (ii) Trade secret information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities; and (iii) Commercial or financial information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities, but only if the source of the information does not customarily disclose it to the public.
(15) Research and development. Information obtained or developed in the conduct of research related to aviation or maritime transportation security activities, where such research is approved, accepted, funded, recommended, or directed by the DHS or DOT, including research results.
(16) Other information. Any information not otherwise described in this section that TSA determines is SSI under 49 U.S.C. 114(s) or that the Secretary of DOT determines is SSI under 49 U.S.C. 40119. Upon the request of another Federal agency, the Secretary of DOT may designate as SSI information not otherwise described in this section.

- **Sensitive Security Information (Agriculture)**

The USDA's Departmental Regulation 3440-2, "Control and Protection of Sensitive Security Information," defines sensitive security information as follows:

Sensitive Security Information means unclassified information of a sensitive nature, that if publicly disclosed could be expected to have a harmful impact on the security of Federal operations or assets, the public health or safety of the citizens of the United States or its residents, or the nation's long-term economic prosperity; and which describes, discusses, or reflects:

(1) The ability of any element of the critical infrastructure of the United States to resist intrusion, interference, compromise, theft, or incapacitation by either physical or computer-based attack or other similar conduct that violates Federal, State, or local law; harms interstate, international commerce of the United States; or, threatens public health or safety;

(2) Any currently viable assessment, projection, or estimate of the security vulnerability of any element of the critical infrastructure of the United States, specifically including, but not limited to vulnerability assessment, security testing, risk evaluation, risk-management planning, or risk audit;

(3) Any currently applicable operational problem or solution regarding the security of any element of the critical infrastructure of the United States, specifically including but not limited to the repair, recovery, redesign, reconstruction, relocation, insurance, and continuity of operations of any element;

(4) The following categories are provided for illustration purposes only as examples of the types of information (regardless of format) that may be categorized as SSI:

1 Physical security status of USDA laboratories, research centers, field facilities, etc., which may also contain vulnerabilities;

2 Investigative and analytical materials concerning information about physical security at USDA facilities such as the above-named facilities;

3 Information that could result in physical risk to individuals;

4 Information that could result in serious damage to critical facilities and/or infrastructures;

5 Cyber Security Information, which includes, but is not limited to:

(a) Network Drawings or Plans
(b) Program and System Security Plans
(c) Mission Critical and Sensitive Information Technology (IT) Systems and Applications
(d) Capital Planning and Investment Control Data (I-TIPS)
(e) IT Configuration Management Data and Libraries
(f) IT Restricted Space (Drawings, Plans and Equipment Specifications as well as actual space)
(g) Incident and Vulnerability Reports
(h) Risk Assessment Reports, Checklists, Trusted Facilities Manual and Security Users Guide
(i) Cyber Security Policy Guidance and Manual Chapters

Monday, October 15, 2012

1412 Dial Court
Springfield, IL 62704

Senator Joseph Lieberman, Chairman
U.S. Senate Committee on Homeland Security & Governmental Affairs
706 Hart Office Building
Washington, DC 20510

Dear Senator Lieberman:

On September 18, 2012 I sent a letter to the Chairman of the US Nuclear Regulatory Commission concerning the NRC's handling of a safety concern regarding Jocassee Dam and the Oconee Nuclear Station. I copied the letter to a member of your Homeland Security & Governmental Affairs Committee staff as well as to the majority and minority staffs of other Senate and House committees who I believed might be interested.

It has been nearly four weeks since I sent my letter and have not heard from either the NRC Chairman's office or the NRC Office of the Inspector General. The only official communication I have received from the NRC was my branch chief informing me that he was directed to fill out a Form 183 for me failing to stamp my 2012-09-18 letter as "Official Use Only – Security-Related Information".

I am reaching out to your committee because I have several concerns which I believe the NRC is incapable of addressing.

For over 18 years the NRC has been aware that the flood wall surrounding the Standby Shutdown Facility at Oconee Nuclear Station is too short to protect the SSF from a failure of Jocassee Dam.[1]

Beginning in 2006[2] (and possibly earlier) staff personnel at the NRC recognized that a failure of Jocassee Dam could result in a nuclear accident at Oconee station.

Although I have seen no documents indicating that there is a security concern associated with the failure of Jocassee Dam, since 2007 all NRC correspondence concerning Jocassee Dam has been stamped "Official Use Only – Safety-Related Information" so it is obvious to me that for at least the past five years the US NRC has believed there is a security concern associated with Jocassee Dam.

---

[1] Letter from Albert F. Gibson, NRC, to J. W. Hampton, Duke, "Notice of Violation and Notice of Deviation (NRC Inspection Report Nos. 50-269/93-25, 50-270/93-25, and 50-287/93-25)," dated February 11, 1994

[2] Letter from Charles Casto, NRC, to Bruce H. Hamilton, Duke, "IR 05000269-06-016, IR 05000270-06-016, IR 05000287-06-016, on 03/31/2006, Oconee Nuclear Station - Preliminary White Finding," dated August 31, 2006

I do not work in nuclear security and I know little about it. It is my understanding that for the commercial nuclear industry the NRC has determined the maximum credible threat with which a nuclear plant might be challenged, and the NRC requires the commercial nuclear reactors which it regulates to adequately guard their plant against such a threat.

It stands to reason that if, as evident from the way the NRC is stamping information regarding Jocassee Dam, there is a credible threat to Jocassee Dam then, because of the danger a failure of Jocassee Dam poses to flooding of the Standby Shutdown Facility at the Oconee Nuclear Station, access to Jocassee Dam should be guarded against the same design basis threat to which the Oconee Nuclear Station and other reactor plants are guarded. I respectfully request that the Senate Committee on Homeland Security & Governmental Affairs verify that the NRC is ensuring access to Jocassee Dam is adequately guarded.

Aside from external terrorist attacks, commercial nuclear reactor plants are required to guard against internal sabotage. Personnel at commercial nuclear facilities are required to receive extensive background checks and, depending on their access to vital areas, are also required to undergo periodic reassessment including interviews with psychologists.

Due to the danger a failure of Jocassee Dam poses to the Oconee Nuclear Station, it stands to reason that the security, operations and maintenance personnel at the Jocassee Dam pumped storage station should be held to the same background checks and periodic reassessments as similar personnel at the Oconee Nuclear Station and other reactor plants. I respectfully request that the Senate Committee on Homeland Security & Governmental Affairs verify that the NRC is ensuring personnel with access to the pump storage plant at Jocassee Dam are adequately screened for insider threats.

As mentioned above, the US NRC decided 5 years ago (since at least 2007) that there is at least enough of a credible security threat to Jocassee Dam to justify withholding from the public all safety related concerns regarding the dam. Although five years is more than enough time to adequately guard Jocassee Dam, the NRC continues to stamp all safety concerns regarding the dam as "Official Use Only – Security-Related Information". This indicates to me that, after five years, the NRC has not been able to adequately ensure the security of Jocassee Dam. This is not surprising to me since the NRC does not regulate Jocassee Dam and therefore has no authority to dictate security measures required there.

As a pumped storage impoundment dam, Jocassee Dam is regulated by the Federal Energy Regulatory Commission (FERC). I know little about FERC, but it is my understanding that FERC does not require the facilities it regulates to be guarded against the same design basis threats that commercial nuclear reactors are guarded against. Although FERC's security requirements are likely adequate for most of the facilities it regulates, in the case of a pumped storage dam whose sabotage is assumed to result in a nuclear accident the only adequate course of action is to require a level of security capable of guarding against a threat equivalent to the design basis threat assumed for commercial nuclear facilities.

Similarly for internal sabotage, FERC's regulations should require that the background checks and periodic reassessments conducted at the Lake Jocassee Dam pumped storage station are equivalent to those conducted at commercial nuclear facilities.

However, I am not sure it is reasonable to expect FERC to be able to treat the Lake Jocassee Dam differently from the other facilities it regulates. FERC might not have the expertise, budget or staffing levels to (1) write the regulations for the Lake Jocassee guard force, (2) periodically inspect the guard force including "Force on Force" exercises, (3) write the regulations for the background checks and periodic reassessments, (4) ensure the background checks were done adequately, and (5) inspect and regulate the periodic reassessment program of the plant personnel including psychological evaluations.

It is apparent to me that during the past five years the NRC has been unable to coordinate with FERC to ensure that the perceived security vulnerability regarding Jocassee Dam has been addressed. Despite this, the three reactors at the Oconee Nuclear Station continue to operate.

In June 2010, the NRC issued Duke Energy a Confirmatory Action Letter (CAL) requiring Duke to upgrade the flood protections at the Oconee Nuclear Station such that by November 30, 2011 the flood barriers adequately protect the equipment at the Standby Shutdown Facility against a failure of Jocassee Dam. This deadline has since been moved to 2016. So for another three or four years Duke Energy is going to be allowed to operate the three reactors at its Oconee Nuclear Station with a perceived security liability unaddressed. This is unacceptable.

If there is truly a security liability posed by Jocassee Dam, Duke Energy can literally address it within hours. Lake Jocassee and Lake Keowee (the lake which Jocassee drains to) are pumped storage impounds. Within a matter of hours, Duke Energy can lower the volume of water impounded by the Lake Jocassee and Lake Keowee Dams such that in the event of a failure of the Jocassee Dam the remaining volume of water impounded will not overtop the inadequately sized flood fall surrounding the Standby Shutdown Facility at the Oconee Nuclear Station.

There is also another solution to the security concern: shut down the three reactors at the Oconee Nuclear Station until the flooding defenses surrounding the Standby Shutdown Facility are adequately improved.

It is understandable that the NRC cannot address the perceived security vulnerabilities at Jocassee Dam since it does not regulate Jocassee Dam. However, the NRC regulates the Oconee Nuclear Station and it is unconscionable that for five years the NRC has suspected a grave security concern and has not addressed it by requiring the three reactors at the Oconee Nuclear Station to be shutdown as long as the volume of water impounded in Lakes Jocassee and Keowee pose a security threat to those reactors. And it is equally unconscionable that the NRC is going to allow this condition to continue for an additional three or four years.

I am not convinced that there is a credible security concern regarding Jocassee Dam. Obviously, all manmade structures can be demolished. But that fact in and of itself does not cause a security threat to exist. For a security threat to exist, the minimum required threat to the structure needs to be less than the maximum credible threat. As mentioned above, the maximum credible threat to the Lake Jocassee Dam is – or should be – assumed to be equivalent to the design basis threat for Oconee Nuclear Station. But what is the minimum required threat to jeopardize the integrity of the dam? Is it a half dozen drunken teenage vandals with some stolen dynamite and a canoe? Or is it a platoon of trained underwater demolition experts from a technologically advanced nation-state?

I do not know enough about dam construction, terrorism or demolition to say what the minimum required threat to Jocassee Dam is. If it is less than (e.g. teenage vandals) or equal to (e.g. a well-armed squad of terrorists) the design basis threat for the Oconee Nuclear Station, then I agree with the NRC that there is a security concern with the Lake Jocassee Dam. If, however, it is greater than the design basis threat for the Oconee Nuclear Station (e.g. underwater demolition experts from the CIA, KGB, Mossad or MI6), then I do not believe there is a credible threat to Jocassee Dam.

I respectfully request the following from the Senate Committee on Homeland Security & Governmental Affairs:

1. Ensure that after five years of assuming there is a security threat to Jocassee Dam, the NRC has adequately assessed the minimum required threat capable of jeopardizing the integrity of the Lake Jocassee Dam.
2. If the minimum required threat capable of jeopardizing the integrity of the Lake Jocassee Dam is greater than the design basis threat for the Oconee Nuclear Station, then request the NRC to cease withholding from the public the correspondence, memos and studies concerning the safety liabilities which a failure of the Lake Jocassee Dam poses to the Oconee Nuclear Station.
3. If the minimum required threat capable of jeopardizing the integrity of the Lake Jocassee Dam is less than or equal to the design basis threat for the Oconee Nuclear Station, then request the NRC to ensure the three reactors at the Oconee Nuclear Station are in a shutdown condition whenever the combined volume of water impounded by the Jocassee and Keowee Dams is great enough to pose a flooding threat to the Oconee Nuclear Station in the event of a failure of Jocassee Dam.

Enclosed with this letter is a list of the correspondence, memos and studies concerning the safety liabilities posed by a failure of the Lake Jocassee Dam. Most of these documents have been stamped by the NRC as "Official Use Only – Security-Related Information" despite not containing any discussion of security concerns. It is my perception that the "security-related" concerns are merely assumed to exist; however it is possible that the NRC has done an actual assessment that shows there is a credible security threat to the dam. If this is the case, then it is unconscionable that in five years the NRC has not done anything to prevent the operation of the three reactors at ONS while an unaddressed vulnerability to their security remains outstanding.

Copied on this letter are several industry groups and government watchdog organizations. There are some within the Nuclear Regulatory Commission who will claim that it is irresponsible for me to share the information in this letter with members of the public. To them I would note that there is nothing in this letter – other than the list of documents enclosed – that is not already public knowledge. With regard to the list of documents enclosed, although these documents are stamped "Official Use Only – Security-Related Information", I do not believe that the mere mention of the existence of these documents constitutes the release of "Security-Related Information".

I have copied politically active organizations on this letter because I believe their participation is vital to the proper functioning of our democratic and republican processes. Although it might not be appropriate to release specific information to these organizations from documents stamped "Security-Related Information", merely informing them that after five years the NRC has failed to adequately address a perceived security threat from the Lake Jocassee Dam is certainly within my rights as a citizen and my duties as a licensed professional engineer.

Very respectfully,

Lawrence S. Criscione

Lawrence S. Criscione, PE
573-230-3959
LSCriscione@hotmail.com

Enclosure – 5 pages

Cc: Senator Susan Collins, Ranking Member, Homeland Security & Governmental Affairs
Senator Richard Durbin, Illinois
Congressman Pete King, Chairman, Homeland Security
Congressman Bennie Thompson, Ranking Member, Homeland Security
Congressman Fred Upton, Chairman, Energy & Commerce
Congressman Henry Waxman, Ranking Member, Energy & Commerce
Chairman Allison Macfarlane, US Nuclear Regulatory Commission
Special Counsel Carolyn Lerner, US Office of Special Counsel
Michael Corradini, American Nuclear Society
Admiral James Ellis, Institute of Nuclear Power Operations
Leslie Barbour, Nuclear Energy Institute
David Lochbaum, Union of Concerned Scientists
Scott Amey, Project on Government Oversight
Louis Clark, Government Accountability Project
Ken Bunting, National Freedom of Information Coalition
Tyson Slocum, Public Citizen Energy Program
Jim Riccio, Greenpeace

List of NRC Correspondence, Memos and Studies Regarding Failure of Jocassee Dam

Date	ADAMS	Title
1994-FEB-11		Letter from Albert F. Gibson, NRC, to J. W. Hampton, Duke, "Notice of Violation and Notice of Deviation (NRC Inspection Report Nos. 50-269/93-25, 50-270/93-25, and 50-287/93-25)," dated February 11, 1994
1994-MAR-14		Letter from J. W. Hampton, Duke, dated March 14, 1994
1994-OCT-6		Internal NRC memo documenting a meeting between Region II and NRR concerning a hypothetical Jocassee Dam failure.
1994-DEC-19		Letter from Albert F. Gibson, NRC, to J. W. Hampton, Duke, "Notice of Violation and Notice of Deviation (NRC Inspection Report Nos. 50-269/94-31, 50-270/94-31, and 50-287/94-31)," dated December 19, 1994
2000-MAR-15		Letter from David E. LaBarge, NRC, to W. R. McCollum, Jr., "Oconee Nuclear Station, Units 1, 2, and 3 Re: Review of Individual Plant Examination of External Events (TAC Nos. M83649, M83650, and M83651)," dated March 15, 2000
2006-APR-28	ML061180451	OCONEE NUCLEAR STATION - INTEGRATED INSPECTION REPORT 05000269/2006002, 05000270/200602, 05000287/2006002
2006-AUG-31	ML080780143	IR 05000269-06-016, IR 05000270-06-016, IR 05000287-06-016, on 03/31/2006, Oconee Nuclear Station - Preliminary White Finding
2006-OCT-5	ML062890206	Oconee, Units 1, 2 & 3 - Response to Preliminary White Finding
2006-NOV-22	ML063260282	IR 05000269-06-017, IR 05000270-06-017, IR 05000287-06-017, Final Significance Determination for a White Finding and Notice of Violation, Duke Energy Carolinas, LLC
2006-DEC-20	ML063620092	Oconee, Units 1, 2, & 3, Appeal of Final Significance Determination for White Finding and Reply to Notice of Violation; EA-06-199
2007-JAN-29	ML070440345	Summary of Revised Fragility Evaluation Results for Jocassee Dam
2007-FEB-5		Letter from Bruce H. Hamilton, Duke, to NRC, "Seismic Fragility Study"
2007-FEB-22	ML070590329	Manual Chapter 0609.02 Appeal Panel Recommendations (Oconee Reply to a Notice of Violation and White Finding (EA-06-199))
2007-MAR-1	ML070610460	Oconee Appeal Panel Review of Manual Chapter 0609.02 Appeal Panel Review of Oconee Standby Shutdown Facility White Finding (EA-06-199)
2007-MAY-3	ML072970510	Oconee, Units 1, 2 and 3 - Request for NRC to Review Appeal of Final Significance Determination for SSF Flood Barrier White Finding
2007-JUN-22	ML071580259	Consideration of New Information Associated with a Final Significance Determination for a White Finding - Oconee NS
2007-JUN-28		Phone call between the NRC and Duke Energy
2007-OCT-1	ML072770765	10/01/2007, Slides with Notes for Final Regulatory Assessment of Oconee Flood Barrier Issue
2007-OCT-1	ML072770775	Dam Failure Information
2007-OCT-1	ML072770777	Questions and Answers Related to Oconee Flood Barrier
2007-NOV-20	ML073241045	Reconsideration of Final Significance Determination Associated with Standby Shutdown Oconee Facility Flood Barrier White Finding
2008-MAY-19	ML081350689	Briefing Package For Drop-In Visit By Duke Energy Chief Nuclear Officer With Chairman Klein And Commissioner Jaczko On May 21, 2008
2008-JUN-23	ML082390669	Proposal for a Risk Analysis of the Failure of the Jocassee and Keowee Dams to Assess the Potential Effects on the Safe Shut Down Facility of the Oconee Nuclear Station, South Carolina
2008-JUL-28	ML082120390	Oconee Nuclear Station - Revisions to the Selected Licensee Commitments Manual (SLC)

List of NRC Correspondence, Memos and Studies Regarding Failure of Jocassee Dam

Date	ADAMS	Title
2008-AUG-15	ML081640244	Information Request Pursuant to 10 CFR 50.54(F) Related to External Flooding, Including Failure of the Jocassee Dam at Oconee Nuclear Station, Units 1, 2, and 3 (TAC Nos. MD8224, MD8225, and MD8226)
2008-AUG-26	ML082390690	Kick Off for Risk Analysis of the Failure of the Jocassee and Keowee Dams to Assess the Potential Effects on the Safe Shutdown Facility at the Oconee Nuclear Station
2008-AUG-28	ML083300427	08/28/2008 - Summary of Closed Meeting to with Duke Energy Carolinas, LLC to Discuss the August 15, 2008, 50.54(f) Letter on External Flooding (TAC Nos. MD8224, MD8225, and MD8226)
2008-AUG-28	ML082550290	Meeting with Duke Energy Carolinas, Oconee Flood Protection and the Jocassee Dam Hazard
2008-SEP-6	ML082250166	Oconee Nuclear Station - Communication Plan for Information Request Related to Failure Frequencies for the Jocassee Pumped Storage Dam (Jocassee Dam) at the Oconee Nuclear Station and Potential Generic Implications
2008-SEP-26	ML082750106	Oconee, Units 1, 2 and 3 - Response to 10 CFR 50.54(f) Request
2008-NOV-5	ML091060761	11/05/08 Summary of Closed Meeting with Duke on External Flooding Issues, including failure of the Jocassee Dam, at Oconee Nuclear Station, Units 1, 2, and 3
2008-NOV-5	ML083390650	11/05/2008 Meeting Slides, "Oconee Site Flood Protection," NRC Meeting with Duke Energy Carolinas, LLC
2008-DEC-4	ML091420319	12/04/2008 Meeting Summary, Meeting to Discuss External Flooding at Oconee Nuclear Station (Reissuance, with Error on Page 3 Corrected)
2008-DEC-4	ML090480044	Oconee Nuclear Station, External Flood NRR Meeting, Rockville, MD, December 4, 2008
2009-FEB-3	ML090280474	Briefing Package for Commissioner Lyons Visit to Oconee on February 4, 2009
2009-APR-6	ML091170104	Oconee Nuclear Station, Units 1, 2 And 3 - Non-concurrence on Evaluation of Duke Energy Carolinas, LLC September 26, 2008, Response to Nuclear Regulatory Commission Letter Dated August 15, 2008 Related to External Flooding
2009-APR-9	ML091030172	Oconee External Flooding Briefing for Commissioner Jaczko
2009-APR-30	ML090570779	Oconee Nuclear Station Units 1, 2, and 3, Evaluation of Duke Energy Carolinas September 26, 2008, Response to External Flooding, Including Failure of the Jocassee Dam
2009-MAY-11	ML092940769	05/11/2009 Summary of Closed Meeting with Duke Energy Carolinas, LLC, to Discuss Preliminary Results of the Recent Inundation and Sensitivity Studies Concerning Failure of the Jocassee Dam and Resultant Flooding at Oconee Nuclear Station, 1, 2, and 3
2009-MAY-11	ML090820470	5/11/2009 Notice of Forthcoming Closed Meeting with Duke Energy Carolinas, LLC, to Discuss Sensitivity Studies Concerning Failure of the Jocassee Dam & Resultant Flooding at the Oconee Nuclear Station, Unit 1, 2, & 3
2009-MAY-11	ML091380424	Oconee Nuclear Station, Slides for Closing Meeting May 11, 2009 with Duke on the Oconee Flooding Issue
2009-MAY-20	ML091470265	Oconee, Units 1, 2 & 3, Request for Extension of Duke Response Time to Referenced Letter
2009-MAY-26	ML091480116	E-mail re Briefing Package for Visit to Jocassee Dam on June 23, 2009
2009-JUN-1	ML091590046	Oconee, Units 1, 2, and 3, Request to Withhold Sensitive Information in Presentation Materials Left with Staff
2009-JUN-10	ML091680195	Oconee, Units 1, 2, and 3 - Interim 30-Day Response to Reference 2.

List of NRC Correspondence, Memos and Studies Regarding Failure of Jocassee Dam

Date	ADAMS	Title
2009-JUN-11	ML091620669	6/11/09 Summary of Closed Meeting with Duke Carolina to Discuss External Flooding at Oconee
2009-JUN-25	ML091760072	NRC Site Visit to the Oconee Nuclear Station on June 15, 2009
2009-JUL-9	ML092020480	Oconee, Units 1, 2, & 3, Final 60-Day Response to Reference 2
2009-JUL-28	ML092230608	Oconee, Submittal of Selected Licensee Commitments Manual SLC Revision
2009-AUG-12	ML090570117	Oconee Flood Protection and the Jocassee Dam Hazard Basis for NRC Allowing Continued Operation
2009-AUG-27	ML092380305	Oconee, Slides for Closed Meeting Regarding External Flood Technical Meeting On August 27, 2009
2009-SEP-25	ML092710344	Site Visit Observation on 09/25/2009 by Joel Munday for Oconee
2009-OCT-28	ML093080034	10/28/09 Slides for Oconee Nuclear Station, Units 1, 2, and 3 - Meeting Slides - External Flood NRC Technical Meeting
2009-NOV-30	ML093380701	Oconee Nuclear Station, Units 1, 2, and 3, Oconee External Flood Analyses and Associated Corrective Action Plan
2009-DEC-4	ML090680737	12/04/09 Summary of Closed Meeting to Discuss the Duke Energy Carolinas, LLC., 09/26/08 Response to NRC's August 15, 2008 50.54(f) Letter on External Flooding at Oconee
2010-JAN-6	ML100280954	01/06/2010 Briefing to the Executive Team on the Oconee Nuclear Station External Flooding Issue
2010-JAN-11	ML100150066	Request Additional Information Regarding the Oconee External Flooding Issue
2010-JAN-15	ML100210199	Oconee, Units 1, 2 and 3 - Additional Information Regarding Postulated External Flood Threat Issues
2010-JAN-29	ML100271591	Evaluation of Duke Energy Carolina, LLC (Duke), November 30, 2009, Response to Nuclear Regulatory Commission (NRC) Letter Dated April 30, 2009, Related to External Flooding At Oconee Nuclear Station, Units 1, 2, And 3 (Oconee)
2010-FEB-8	ML100470053	Oconee, Units 1, 2, & 3, External Flood, Response to Request for Additional Information
2010-FEB-26	ML100610674	Oconee, Units 1, 2, & 3, External Flood Revised Commitment Letter
2010-MAR-5	ML103430047	Oconee Nuclear Station, Units 1, 2, & 3, Letter From Duke Energy Carolinas, LLC Regarding External Flood, Response to Request For Additional Information
2010-MAR-15	ML100780084	Generic Failure Rate Evaluation for Jocassee Dam Risk Analysis
2010-MAR-18	ML100810388	Prepare Briefing Book and Material for Eric Leeds for the Duke Fleet Meeting on March 18, 2010
2010-APR-14	ML100760109	Generic Failure Rate Evaluation for Jocassee Dam
2010-MAY-27	ML101600468	Oconee, Units 1, 2 & 3, Response to Requested Information on the Protection Against External Flooding Including a Postulated Failure of the Jocassee Dam
2010-JUN-1	ML101750619	OUO - Communication Plan For Issuance of Confirmatory Action Letter To Duke For Oconee - External Flooding June 2010
2010-JUN-3	ML101610083	Oconee Nuclear Station, Units 1, 2, and 3, - External Flood Commitments
2010-JUN-22	ML101730329	Oconee, Units 1, 2 & 3, Confirmatory Action Letter (CAL 2-10-003), Commitments to Address External Flooding Concerns
2010-JUN-29	ML101890803	06/29/2010 Summary of Closed Meeting With Duke Energy Carolinas, LLC, to Discuss External Flooding at Oconee
2010-JUL-7	ML101880768	OUO - IR 05000269-10-002, 05000270-10-006, 05000287-10-006; 01/01/2010 - 03/31/2010; Oconee Nuclear Station Units 1, 2 and 3; Interim Compensatory Measures for External Flood
2010-JUL-19	ML101900305	Identification of a Generic External Flooding Issue Due to Potential Dam Failures

List of NRC Correspondence, Memos and Studies Regarding Failure of Jocassee Dam

Date	ADAMS	Title
2010-AUG-2	ML102170006	Oconee Units 1, 2, & 3, Response to Confirmatory Action Letter (CAL) 2-10-003
2010-OCT-20	ML102910480	NRC Assessment of Oconee External Flooding Issue (October 18, 2010)
2010-OCT-26	ML102990064	NRC Staff Assessment of Duke Energy Carolinas, LLC, Oconee External Flooding Issue (TAC NOS. ME4441, ME4442, and ME4443)
2010-NOV-29	ML103490330	Oconee Nuclear Site, Units 1, 2, and 3, Oconee Response to Confirmatory Action Letter (CAL) 2-10-003
2011-JAN-5	ML110180609	Enclosure 1, Oconee Nuclear Station, Major Project Plans
2011-JAN-10	ML110260443	Non-concurrence on Oconee Assessment Letter
2011-JAN-28	ML110280153	Staff Assessment of Duke's Response to Confirmatory Action Letter Regarding Duke's Commitments To Address External Flooding Concerns At The Oconee Nuclear Station, Units 1, 2, And 3 (ONS) (TAC NOS. ME3065, ME3066, and ME3067)
2011-MAR-5	ML103410042	Supplement to Technical Basis for Allowing Oconee Nuclear Station to Remain in Operation Through November 2011, Associated with the External Flooding Issues
2011-MAR-15	ML110740482	Analysis Report for the Proposed Generic Issue on Flooding of Nuclear Power Plant Sites Following Upstream Dam Failures
2011-APR-29	ML111460063	Oconee Nuclear Site, Units 1, 2, and 3, Response to Confirmatory Action Letter (CAL) 2-10-003
2011-AUG-16	ML11229A710	E-mail re Briefing Package for Visit to Oconee Nuclear Power Plant on September 12-13, 2011
2011-AUG-18	ML11174A138	Oconee Nuclear Station, Units 1, 2, and 3, Assessment of Duke Energy Carolinas, LLC April 29, 2011, Response to Confirmatory Action Letter Regarding Modifications to Address External Flooding Concerns (TAC Nos. ME6133, ME6134, and ME6135)
2011-AUG-31	ML112430114	Screening Analysis Report for the Proposed Generic Issue on Flooding of Nuclear Power Plant Sites Following Upstream Dam Failures
2011-SEP-1	ML11244A024	Briefing Package for Visit to Oconee Nuclear Power Plant on September 12-13, 2011
2011-OCT-3	ML11278A173	Oconee Nuclear Station (ONS), Units 1, 2, and 3, Response to Requests for Additional Information Regarding Necessary Modifications to Enhance the Capability of the ONS Site to Withstand the Postulated Failure of the Jocassee Dam
2011-OCT-17	ML11294A341	Oconee Nuclear Station (ONS), Units 1, 2, and 3, Response to Requests for Additional Information Regarding Necessary Modifications to Enhance the Capability of the ONS Site to Withstand the Postulated Failure of the Jocassee Dam
2011-DEC-16	ML113500495	Screening Analysis Report for the Proposed Generic Issue on Flooding of Nuclear Power Plant Sites Following Upstream Dam Failures_redacted
2012-JAN-26	ML12026A549	Briefing Package for Commissioner Svinicki Visit to Oconee on February 1, 2012
2012-JAN-31	ML12026A254	Communication Plan for Oconee Nuclear Station (ONS) Following Issuance of GI-204
2012-FEB-3	ML12039A239	Oconee, Units 1, 2 and 3 - Request for Withholding from Public Disclosure Duke Energy Letter Dated May 20, 2009 Involving Postulated Failure of the Jocassee Dam
2012-FEB-9	ML12039A217	Briefing Package Request for Meeting with Duke Energy on February 16, 2012

List of NRC Correspondence, Memos and Studies Regarding Failure of Jocassee Dam

Date	ADAMS	Title
2012-FEB-17	ML12053A016	Duke Energy Carolinas, LLC - Recommended Revisions to the Oconee Nuclear Station Section of NRC's Screening Analysis Report for the Proposed Generic Issue on Flooding of Nuclear Plant Sites Following Upstream Dam Failure
2012-FEB-23	ML12058A236	02/23/12 Summary of a Teleconference between the US NRC and Duke Energy Regarding Comments made by Duke Energy Concerning the Issuance of the Screening Analysis Report for Generic Issue 204
2012-MAR-5	ML090510269	NRC Information Notice 2012-002 Potentially Nonconservative Screening Value For Dam Failure Frequency In Probabilistic Risk Assessments
2012-MAY-15	ML12129A186	Oconee Nuclear Station, Units 1, 2, and 3 - Request for Additional Information Regarding Modifications to Address the External Flooding Concerns (TAC NOS. ME7970, ME7971, AND ME7972)
2012-JUN-14	ML12167A372	Oconee, Units 1, 2, and 3, Response to Requests for Additional Information Regarding Modifications to Address External Flooding Concerns
2012-JUL-11	ML12215A327	07/11/2012 Licensee Non-Public Meeting Slides on Oconee External Flood Mitigation
2012-JUL-11	ML12188A071	Briefing Package for Meeting with Duke Energy on July 11, 2012
2012-AUG-7	ML12206A325	Briefing Book for Meeting with Duke Energy on August 7, 2012
2012-SEP-20	ML12268A404	Communication Plan for Flooding September 2012
2012-SEP-20	ML12219A163	Oconee Nuclear Station, Units 1, 2 and 3 - Response to Questions Regarding Modifications to Address External Flooding Hazards (TAC Nos. ME7970, ME7971, AND ME7972)