washingtonpost.com

Nuclear Security Decisions Are Shrouded in Secrecy

Agency Withholds Unclassified Information

By R. Jeffrey Smith
Washington Post Staff Writer
Monday, March 29, 2004; Page A21

Nineteen men in four squads. That's the size of the terrorist threat that some nuclear critics say armed guards at U.S. nuclear power plants and weapons facilities should be able to rebuff.

The figure is pegged to the Sept. 11, 2001, al Qaeda assaults on the World Trade Center and Pentagon. The Bush administration has updated a much weaker 1980s-era standard, but government and congressional officials say the presumed attack still involves considerably fewer than 19 terrorists -- and that means requiring a smaller guard force than critics say is necessary.

A legal dispute related to this standard has now arisen, but -- as in other recent discussions of the administration's response to terrorism threats -- the squabbling is occurring almost entirely outside public view. The immediate issue is an unclassified request by a nuclear power plant operator for an exemption from certain parts of the new security requirements.

The Nuclear Regulatory Commission has deemed the operator's request sensitive, and declared that its release would bring criminal prosecution. Critics who allege the standards are already too lax have filed a challenge to the exemption request, which the commission has also declared is too sensitive to be released.

It is but one example of the manner in which post-Sept. 11 anti-terrorism controls -- even those concerning unclassified information -- have altered the landscape of public debate about security matters. Civil defense arrangements that were once the subject of mostly open rulemaking or debate are now often decided under a cloak of secrecy covering all but industry and government participants.

The result has been to complicate efforts to hold officials accountable for their decisions, especially in the counterterrorism field, say advocates of open policymaking. "There has been a proliferation of new controls on unclassified information," said Steven Aftergood, director of the Government Secrecy Project at the Federation of American Scientists. "This is where the public is at a disadvantage," because few mechanisms are available to challenge these controls or to ensure that public representatives have access comparable to what industry routinely gains.

In the nuclear site security case, Duke Power asked the NRC to waive certain security precautions, normally required wherever more than a bomb's worth of special nuclear materials are present. The request involves the planned shipment next spring of French-made nuclear fuel rods containing plutonium to its plants in North and South Carolina, where they will be stored

and then burned in reactors.

The challenge has been filed by the Blue Ridge Environmental Defense League, with technical advice from the Union of Concerned Scientists. Although UCS scientist Edwin Lyman, who has a security clearance, read the exemption request after signing a non-disclosure statement, neither he nor the environmental group has been able to learn exactly what the NRC's security standards are.

Lyman says he is willing to keep whatever he learns confidential, but that without knowing more, he cannot fully assess the proposal or effectively express concerns about the underlying standard. But the NRC, ruling in a Feb. 18 decision, said that although Duke Power has a "need to know," the environmental group does not.

Rep. Edward J. Markey (D-Mass.), a longtime critic of nuclear power, has complained that the NRC barred the groups from learning the same information it shared not only with Duke Power but also with the Nuclear Energy Institute, an industry group that has lobbied against stiffer guard force requirements.

In a March 18 letter to the NRC, institute President Joe Colvin said the group was meeting "almost daily" with the commission staff to discuss the security standard, now undergoing a final government review. A senior NRC official, speaking on condition that he not be named, asserted that "the public does not have a need to know [the postulated terrorist threat] and doesn't, for the most part, have security clearances. . . . There is no way you can bring the public into that discussion." He said the critics "are unlikely to have anything but disdain for anything that we do, so I don't know what we can gain from that." Duke Power maintains that its power plants are well protected, and that its security exemption request is reasonable, given the difficulty of diverting plutonium contained in the bulky fuel rods. Nuclear Energy Institute Vice President Steve Floyd is skeptical of the critics' demands for even controlled access to threat information. "You have to realize what their agenda is -- to drive costs up to the point where nuclear [power] is no longer feasible," Floyd said.

But Aftergood of the Government Secrecy Project said that "it is the public that has to deal with the consequences" of a nuclear site security breach, and so it is entitled to participate more fully in the debate. "Fundamentally, the NRC policy views members of the public as a threat," Aftergood said.

The NRC is not alone in imposing its own, new controls on unclassified information. The Department of Homeland Security has promised not to disclose security data furnished by companies on their "critical infrastructure or protected systems," a potentially broad category of data.

The Federal Energy Regulatory Commission has adopted a slightly different policy to shield what it calls critical "energy infrastructure" data: It will release the data to recipients who sign a non-disclosure pledge. These and other government offices are essentially taking their cues from a White House directive in March 2002, which encouraged government officials to treat all unclassified security-related information as sensitive data not subject to public release.

But the NRC policy is one of the most expansive. The commission recently threatened staff

members at a watchdog group, the Project on Government Oversight (POGO), with criminal prosecution because they published their own detailed critique of security at Entergy Nuclear's two reactors at Indian Point in New York.

"The Commission is concerned that a public discussion of some of those issues would not be in the best interests of the United States," NRC Secretary Annette L. Vietti-Cook wrote to the group in the fall, noting problems related to discussion in the critique of the number of attackers a plant might have to fend off and particular security weaknesses.

Roy P. Zimmerman, director of the NRC's office of nuclear security, subsequently wrote that POGO's critique -- which the group says was based solely on interviews it conducted with people who participated in or observed Indian Point security drills -- had been deemed "safeguards information" protected by federal law. Such laws, he noted, apply to "any person . . . who produces, receives, or acquires" such data, no matter how they got it.

In an apparent Catch-22, Zimmerman said the commission could not, however, specify what information it wanted deleted from the critique. That prompted POGO's lawyer, David C. Vladeck, to allege that the NRC was trying to "silence" the group. Eventually, the NRC, which denied the accusation, agreed to describe the offending information in general terms, and POGO released a new critique containing passages it had rephrased.

But, in an illustration of the challenges the government faces in trying to quash public discussion of sensitive but unclassified information, the original POGO critique remains posted on an independent Web site devoted to disseminating whatever officials seek to censor (**www.thememoryhole.org**).

Since Sept. 11, 2001, many bureaucrats have been using heightened security concerns to "hide their inadequacies," said Danielle Brian, POGO's executive director. "It has gone far, far beyond what is reasonable."

Aftergood similarly warns that the government has "cast too broad a net and . . . failed to provide an internal self-check." The sole office for policing the government's disclosure of security-related information was created in an era when data were either classified or subject to public release, and has no jurisdiction over the burgeoning realm of sensitive but unclassified information, he said.

J. William Leonard, who heads that office -- the Information Security Oversight Office, an arm of the National Archives -- confirms Aftergood's account. Although making no comment on specific disputes, he said that in many instances, "sensitive but unclassified" is a label without meaning that is misused by officials who lack the proper "training, background or understanding" to decide what to withhold. Leonard said that strictly applying a "need to know" test can sometimes exclude important players whose valuable insight is not foreseen.

Leonard gave a speech last year that he says is still relevant, in which he noted that the government needs to create "a seamless process" for sharing or withholding information, yet "we are . . . quite possibly adding new seams every day" by not enforcing a reasonable, government-wide policy.

Watchdog groups that have raised questions about Duke Power's request for a waiver of security requirements have been frustrated by the secrecy surrounding the deliberations. Above, Duke's McGuire Nuclear Station in North Carolina, which recently tightened security programs.

Photo Credit: David T. Foster III -- Charlotte Observer