



# International Environmental Law Committee Newsletter

## **Avoiding Liability from Security Mandates and Regulators with Integrated Management Systems**

*Michael Penders*

President

Environmental Security International

[www.esisecurity.com](http://www.esisecurity.com)

International security mandates, guidelines, and regulatory requirements over the last three years have added complexity to the job of maintaining compliance at significant manufacturing facilities and those considered a part of critical infrastructure. This is particularly the case for corporations and facilities involved in international trade of goods that may pose harm to human health or the environment if not managed in a safe and secure manner from the full range of generation, transport, use at a facility, and environmentally sound recycling or disposal of hazardous wastes.

Before September 11th, it was difficult enough for corporate managers and counsel to manage compliance with the broad array of requirements from an equally broad array of regulatory bodies on the state, local, federal, and international levels, including dozens of agencies involved in regulating trade at ports alone. Advances in environmental management systems in the last eight years have helped firms manage compliance, and indeed move beyond compliance to models of continuous improvement, pollution prevention, and inherently safer systems. Such systems, however, are only as good as the targets and objectives agreed to, and only then if implementation meets performance goals on a continuous basis.

To the extent that management systems conforming to standards such as ISO 14001, ISO 17799, BSI 18001, NFPA 1600, among others, included in their targets and objectives processes for assuring compliance with all legal requirements (which of course they must to manage risk in a credible manner), they marked important milestones as international standards..

What any of these standards alone failed to do, however, was address risk in a comprehensive or integrated manner. They could not provide managers or counsel with a means to prioritize relative risks in a meaningful way for business continuity, or provide a basis for the “Strategic Sustainability” of the business itself.

These failures are understandable for at least two principal reasons: (1) these standards tend to deal with only one set of compliance or other issues in a segregated fashion with no consideration or prioritization of overall risks to a facility or corporation; and (2) while standards like ISO 14001, and compliance with the environmental laws themselves, may focus on addressing the general risks inherent in managing goods and processes that impact the environment and health, what they fail to address in a serious way are risks from deliberate acts or attacks from within or outside the facility.

Of course, after September 11th, the risk calculus and thus the liability framework was altered for the foreseeable future. No longer could a deliberate attack on a facility, its supply chain, or infrastructures be considered outside the scope of “reasonably foreseeable” events. Indeed, everyone is on notice of terrorist plans to use chemical or other facilities that manage hazardous materials as weapons of destruction.

Moreover, the proliferation of security mandates, such as the guidelines and code adopted by the American Chemistry Council (ACC), and new regulations such as those set forth following the Maritime Transportation and Security Act of 2002, establish the basis for liability should a compliance problem or other event occur while these standards or requirements have not been met.

The good news is that all of these considerations are driving a more integrated approach to environmental and security assessment that is in turn moving the paradigm of management systems towards a more comprehensive risk management regime. Some critical infrastructure facilities required to conduct Vulnerability Assessments, have combined that with a gap analysis or audit of environmental, health, safety, information, and security management systems.

Several such facilities have now used those findings as the basis for adopting a Security Management Systems (SMS) approach. A SMS integrates the features of systems designed to manage one set of compliance issues or goals within a management systems approach to include other functions that are most important to the overall security of the operations, weighted toward addressing areas of greatest risk first.

For example, one of the largest wastewater treatment systems in the world recently completed an environmental security audit, combining an internal investigation into acts of sabotage with an environmental compliance audit, as well as a vulnerability assessment. This facility has now begun the process of implementing a Security Management System, designed to incorporate the most significant aspects of several ISO management systems standards, focused on achieving the overall security (as well as environmental performance) goals of the facility.

Other facilities adopted integrated assessment methodologies after they recognized the need to audit or upgrade one or more systems, and elected to do so in a more comprehensive way to address security concerns as well. Significantly, this integrated approach allows identification of areas where efficiencies resulting from bringing different systems together may realize cost, energy, and natural resource savings.

In fact, significant savings have been demonstrated at several military bases that opted for a security focused EMS to meet recent mandates from DOD and the federal government to adopt environmental management systems at all federal facilities. These military bases have been recognized on the state and national levels for their leadership in environmental performance and efficiency.

This integrated approach to environmental management and security has received attention in a number of quarters, such as the ACC's Responsible Care and Security Code., and is beginning to find its way into international standards. For example, last August in Tel Aviv, a group of experts in environmental management, security, and standards from the United States and Israel convened to define and draft a new international standard for Security Management Systems.

This process was initiated by the United States/Israel Science and Technology Foundation (see [www.usistf.org](http://www.usistf.org)) which has now initiated a series of pilot projects at critical infrastructure facilities in the US and Israel to assess this draft international standard for Security Management Systems (SMS). The draft international standard is designed to be consistent with existing standards for environmental, health, safety, information, emergency response, and disaster recovery management systems, as well as physical security guidance.

A SMS then seeks to integrate the most important elements of these mostly segregated functions at most facilities into a single management system focused on security and the reduction of risks from deliberate acts within or outside a facility.

These pilot projects at petro-chemical plants, water treatment facilities, ports, aerospace facilities, and hospitals in the U.S, and Israel are designed to test this integrated management systems approach and develop data about the utility and performance of such a Security Management System, before the draft international standard is finalized. After implementation, these systems will be tested to determine how quickly the overall system, or any of its constituent parts, can detect, prevent, to limit the consequences of an event that disrupts or threatens the facility, or its compliance status.

In another indication of growing international recognition of such an approach, and implications for international trade, Italian Senators and Italy's Parliamentary Waste Commission agreed last summer to support the import of US plasma technologies to treat hazardous and other wastes at a conference at the American Embassy in Rome. They premised their approvals on the condition that these technologies be deployed within the context of a Security Management System.

In his concluding remarks, the President of the Italian Senate emphasized the importance of management systems that could demonstrate the safety and security of treating hazardous wastes with these environmentally advanced technologies. He stressed the system was as important as the evaluation of the technology for receiving expedited approvals on the regional and national levels to address the waste emergencies in Italy.

In this way, a security management system that demonstrates performance with respect to safety, security, and regulatory compliance represents a risk management tool that is credible and transparent enough to receive international recognition necessary for trade, as well as financial and insurance consideration. While ISO 14001 and other standards have received consideration for some trade purposes, they have not received much, if anything, in the way of financial consideration, in part, because they are not performance based, do not even address regulatory compliance in a transparent manner, and have not established themselves as credible risk management measures.

On the other hand, a Security Management System that explicitly prioritizes risks and reduces them in a comprehensive and performance based model, represents a significant risk management measure and tool. It also provides many more stakeholders the basis for making favorable decisions for facilities and corporations across a broad range of regulatory, public, and financial institutions from which they seek consideration.

## **Conclusion**

Increasingly, organizations that are subject to various regulations, security mandates, and attendant liability concerns, are concluding that a security focused approach to management systems makes good business sense. That is, if management must conduct an audit or seeks certification for one or more management systems' standards, why not broaden the scope to cut across the different operational functions most important from security and international trade perspectives? Management may then develop a system that allows it to focus resources on the areas of greatest risk.

Certification of a management system that addresses environment, health, safety, as well as information, emergency response, disaster recovery, and security is more valuable than certification

as to anyone of these areas. Moreover, with the overall risk management perspective that an integrated assessment allows, managers may make improvements where needed most, and proceed with certifications for discrete aspects of the system, such as environmental or information systems, as they become a requirement or focus of customers or other stakeholders.

As the basis for liability has shifted to security risks, implementation of an empirically based management system allows managers to dedicate resources to those risks first. Such an approach should serve to protect the entity from liability from wherever it may emerge, particularly if counsel can represent these processes as voluntary efforts that go beyond the narrow and segregated requirements of existing regulations and policies.

A leading performance measure for a Security Management System is how quickly managers can detect, prevent, and/or limit the consequences of deliberate or negligent acts from within or outside a facility. Only a system that spans various operational and compliance functions, physical site, information, and supply chain security, can address those real performance measures critical to protecting corporate assets, assuring business continuity, and minimizing liabilities., including those related to compliance issues.

Implementing management systems that fail to provide protection from deliberate acts, or liability from such acts after they are foreseeable, may not be cost effective, particularly if they address only one set of compliance issues. If enhancing security is also an important objective, or a legal mandate, for a client, a Security Management System may be tailored to address their priorities and risks, and reduce liability from a number of fronts in a post September 11<sup>th</sup> world.

\*\*\*\*\*

Michael Penders, an attorney who was formerly Director of Legal Counsel at EPA's Office of Criminal Enforcement, is President of Environmental Security International, which conducts integrated assessments and designs Security Management Systems and is participating in the United States/Israel Science and Technical Foundation pilot projects, [Mpenders@esisecurity.com](mailto:Mpenders@esisecurity.com).