BNL-101359-2013-IR

NONPROLIFERATION AND KNOWLEDGE SECURITY TRAINING

Global Security Through Science Partnerships

DRAFT

Notice: This manuscript has been authored by employees of Brookhaven Science Associates, LLC under Contract No. DE-AC02-98CH10886 with the U.S. Department of Energy. The publisher by accepting the manuscript for publication acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or any third party's use or the results of such use of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof or its contractors or subcontractors. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Knowledge Security

- **Module 1; Introduced the concept of knowledge security related to dual use technology and threats**
- **Module 2: Provided more details of dual use concepts and treaties specific to biological, chemical, nuclear and missile technologies**
- **Module 3 will introduce responsible science and its role in knowledge security, and methods of protecting knowledge**

MODULE 3

Recognizing and Responding to Elicitation/Solicitation

Module 3 Objectives

- **Inform and create awareness about <u>protecting</u> dual use knowledge**
- **Knowledge is in two forms**

  Intangible-What scientists/engineers know

  Tangible-Information in physical/digital form
- **Knowledge can be obtained by adversaries through direct or indirect means; from individuals and organizations.**
- **Protecting critical <u>knowledge</u> at one place is easier and will enhance security every where.**

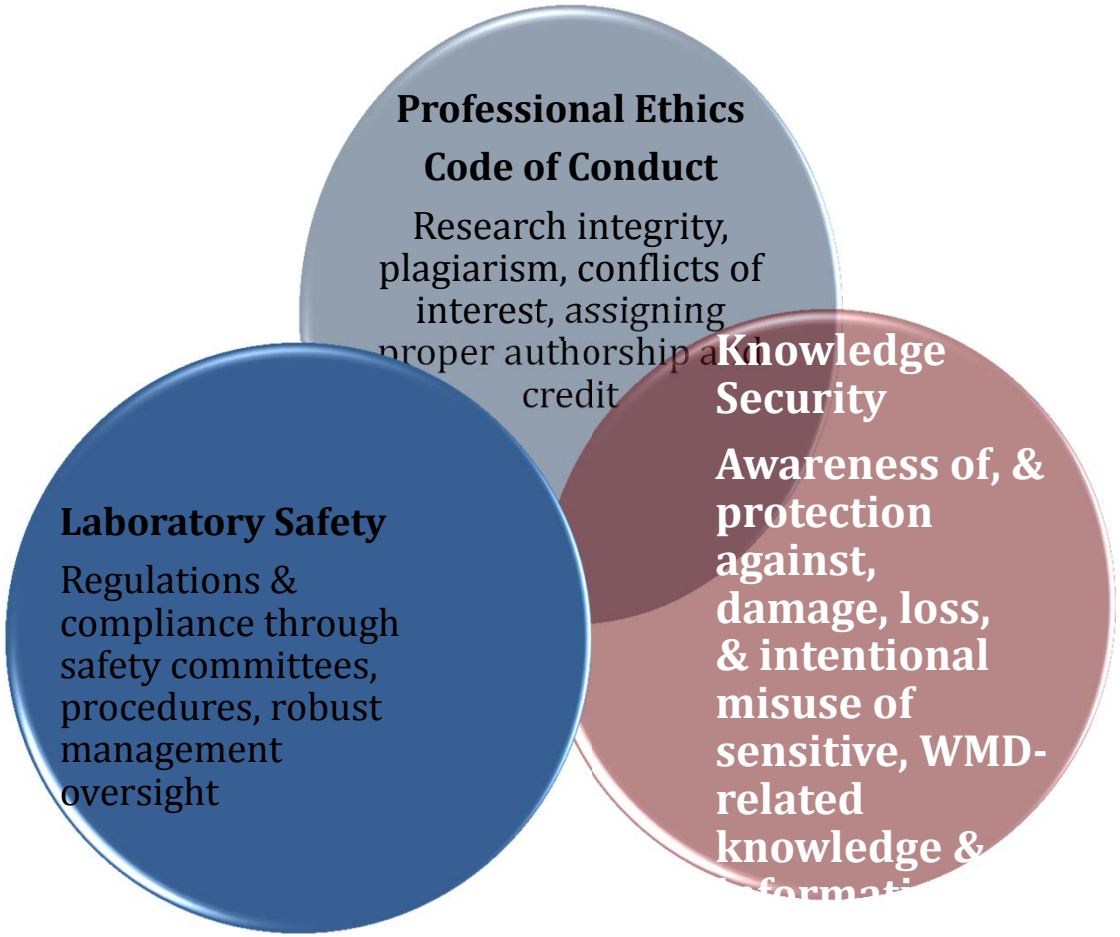
Module 3: Outline

1. **Responsible Science; ethics and Codes of Conduct**
   - Brief intro to scientific ethics-where knowledge security fits
   - Historic codes involving scientists
   - Types of codes, pros cons
   - Contemporary activities- UK initiatives- ***place for leveraging materials?***

2. **Processes to Safeguard Information**
   - Physical Protection of Information
   - Method of protecting Knowledge
   - Establishing Oversight Personnel
   - Parallels to related scientific regulatory regimes

3. **Group Discussion and Exercises**
4. **Introduction WEB based resource center**

3.1 Responsible Science- Three Elements



3-1; Responsible Science

- **Responsible science provides a starting point for awareness of dual use knowledge**

- **Protection of intangible form of knowledge; This is the form of knowledge that scientists/engineers have acquired during the course of education, training, job and research**

- **Ethics and Code of conduct are part of responsible science that will guide protection of <u>intangible</u> form of knowledge from being misused**

3.1; Role of Safety in Science

- **<u>Safety</u> is <u>security</u> of colleagues and neighbors of the organizations**
- **<u>Safety</u> is being incorporated in responsible science;**
- **Procedures and materials to be handled in safe manner with proper protection for the scientists and neighbors.**
- **Safety is personnel conduct**
- **Institutional compliance through safety committees , procedures**
- **Management emphasis-Role of leadership**
- **Knowledge security culture can have path similar to safety culture.**

3.1: Ethics and Code of Conduct

- **Ethics is personal responsibility that scientists have based on inherent value system, senior colleague role model, and guidance of the profession**
- **Code of Conduct; These are rules and guidance that are created by institutions and professional societies to be followed in course of scientific activities**
- **Ethics and Code of conduct can include safeguarding dual use knowledge**

3.1 Ethics in Science

- **Honesty in research**
- **Avoid fabrication of data,**
- **Avoid Plagiarism,**
- **Avoid Conflict of interest and**
- **Give proper credit.**
- **Knowingly do no harm with implication to dual-use knowledge protection**

3.1: Honesty

- **Research misconduct is a world-wide problem that impacts more than the researchers involved. Our quality of life is increasingly dependent upon the quality of our science.**
- **False data offers false hope to anyone looking to science for a solution. Physical harm can result when falsified data become the basis for medical treatment or design of infrastructure. Misconduct impacts people's lives.**
- **The other aspect of honesty is to conceal harmful aspect of results of research from public**

Applied Ethics-Field Specific

- **There are various fields of applied ethics:**
  - Medical ethics
  - Environmental ethics
  - Research ethics
  - Bioethics
  - Engineering Ethics

- **Some of these fields can guide towards agreed ethical position on dual-use knowledge**

- **Few Examples of Ethics**

From Applied Medical ethics…

- **It includes ideas about:**
  - the sanctity of human life
  - power to end life
  - power to enhance life
  - power to interfere with life processes

- **Defines relationships between researchers and the public and among fellow-researchers**
- **Guidance of protecting life/health from misuse of dual use science**

From Applied Environmental ethics….

Ideals about:

- **conservation of the world as we know it**
- **preserving life quality for humans and non-humans**
- **And the intrinsic value of the environment**
- **Protect environment from misuse of dual-use science**

From Ethics for Engineers

- **Using their knowledge and skill for the enhancement of human welfare;**
- **Shall hold paramount the safety, health and welfare of the public in the performance duties of their professional.**
- **Being honest and impartial, and serving with fidelity their clients (including their employers) and the public; and**
- **Shall respect the proprietary information and intellectual property rights of others,**
- **Striving to increase the competence and prestige of the engineering profession.**
- **Prevent dual-use expertise/knowledge from harming society**
-

http://files.asme.org/STLLC/13093.pdf

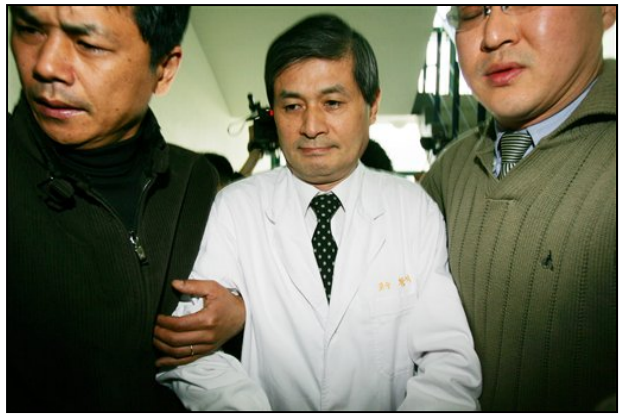
From Applied Biomedical research ethics….

- **Guidance;**
  - Privacy, anonymity and confidentiality
  - Autonomy, consent, right to information
  - Expectancy of creating no harm
  - Reasonable requirements of benefit
  - Expectations of the reasonable publication of work
  - Maintaining dual use knowledge as reasonably harmless and restricted

Case Example: Applied bioethics….

- **Ideals of how to consider the impact of new technology and knowledge on people**
- **Recognition of the uses and limitations of technology on life**
- **Recognition of potential misuse of dual-us biotechnologies**

Case of Misconduct-Fabrication



Woo-suk faces a maximum sentence of life in prison.

January 2006 - Dr. Hwang Woo Suk, the South Korean researcher who claimed to have cloned human cells, fabricated evidence for all of that research, according to a report released by the Seoul National University investigating panel. The finding strips any possibility of legitimate achievement in human cell cloning from a researcher who had been propelled to international celebrity and whose promise to make paralyzed people walk had been engraved on a Korean postage stamp.

May 2006 - Scientist Hwang Woo-suk was indicted on charges of embezzlement, fraud, and bioethics violations in a scandal over faked stem cell research that shook the scientific community and embarrassed the government of South Korea. Five members of Hwang's research team were also indicted.

May 2006 (Associated Press), Jan. 2006 (*New York Times*)

Common Points in All of the fields of Applied Ethics

- Relationships of power
- Rights of individuals (rather than populations)
- Notions of responsibility on one or more sides
- ***Attempts to define rules or guidelines to prevent harm***
- A lack of accurate, definite predictions of outcomes

Applied Ethics: dual-use

- Relationships among various stakeholders- BETWEEN scientists and authorities, Among scientists, BETWEEN scientists and the public
- Rights of individual scientist AND populations
- Responsibility to the wider world
- Attempts to define rules or guidelines to prevent harm – TO AVOID or MINIMISE dual-use risks

Introduction of Ethics of dual-use

- **Introduce these ideals in suitable places and times, to all scientists:**
  - In education contexts-Universities
  - In work contexts-Institutions
  - In peer-review and sharing contexts
  - In global contexts

Knowledge protection begins with the individual scientist

- **Our process MUST begin with individual scientists**
  - Educating ourselves to become aware of dual-use issues and risks of sharing certain kinds of information
  - **This is the goal of this course**

- **Once scientists are equipped with this knowledge, they can become knowledge security advocates, and address dual-use issues within larger contexts**
  - Research groups
  - Institute/university
  - Country
  - International/global community of scientists

In universities

- **By tackling these important issues in the educational context, scientists can consider dual-use-issues from an early stage of their careers**

- **Universities provide a relatively safe, unpressured environment**

- **Develop an ethical philosophy on which to base their future work**

As Professionals

- **To recognise and takes steps to minimise the risks of dual-use of technological advances, such as:**
- **Changes in research practice – access to data, analysis and interpretation**
- **Which may raise issues for individual scientists or research groups**
- **Which may require support from external groups**

In peer-sharing contexts

- **Information sharing is an important part of scientific research.**

- **Reducing the risk of dual-use of science developments may involve:**

  - Changes in peer communications

  - Changes in conference practices – access to sessions, curtailed paper and online publications after meetings

  - Changes in journal publication practices, selectively publishing low-risk and not publishing high-risk research

Expertise Proliferation: Practical Rules for Scientists

- **What to look out for…**
  - Recognizing different threats
  - maintaining a questioning attitude without impacting routine work activities
  - developing skills to address scenarios, that could raise concern
  - Develop some good responses if you suspect you're being solicited for information
  - Be vigilant about theft of information

MODULE 3.1.2 Code of Conduct

Module 3.1.2; Scientific/Technical Codes of Conduct

- Different forms and Sources of Codes of Conduct
- Defines standards of professional conduct, of those working in science medicine, accounting, and other engineering professions, as a mechanism for setting and encouraging reflection.
- Codes could include knowledge security
- Type:
  - aspirational values,
  - educational/advisory guidelines, or
  - enforceable requirements such as in the workplace.

Module 3.1.2; Scientific Codes of Conduct

- Aspirational codes: (Example Chemistry)
  - Set out ideals that practitioners are expected to uphold, such as standards of research integrity or honesty. These may be realistic or idealistic. For instance, in 1965 the American Chemical Society approved the Chemist Creed, which called for each chemist 'to be a faithful and incorruptible agent, respecting confidence, advising honestly, and charging fairly'.

Module 3.1.2; Scientific Codes of Conduct

- Educational/advisory codes:
- Provide more detailed guidelines for appropriate action. Enforceable codes go further still by embedding standards within wider systems of regulation where they can be made obligatory. The 1963 Code of Ethics of the American Institute of Chemical Engineers provided a variety of rules for its members, such as: 'He will not disclose information concerning the business affairs or technical processes of any present or former employer or client without his consent.' Failure to comply with this Code could have lead to professional or, in some cases, legal sanction.

Module 3.1.2; Scientific Codes of Conduct

- Enforceable codes
  - These are codes that are prescribed and require compliance with consequences. However, here it is often argued that ethical decisions cannot be reduced to merely following 'inert' rules and formulae which do not address the complexities of situations.

MODULE 3.2 PROTECTING KNOWLEDGE

Knowledge Protection

- **Expertise requires**
  Knowledge on how to use information
  Information in form of different media

- **Protection of knowledge will require protection of information**

- **Next few sections are based on regular training provided to scientists/engineers at Brookhaven National Laboratory**

- **Brookhaven National laboratory has oversight structure, and procedures to support scientists with issues of dual use technology/export**

Module 3.2; Processes to safeguard information

- **Establish procedures for tangible form of information**
  - Print Media
  - Digital Media
  - Transmission
- **Establishing oversight personnel**
  - Self-monitoring,
  - site Point of Contact
  - peer review system,
  - implement through an established University/Institutional Review Board.
  - **These concepts will be developed further in next few slides.**

Information Protection

- **Information/knowledge is created, stored and transmitted in digital form**
- **Storage, network and communication and dissemination**
- **Some Ideas on Information protection**
  - Back Up Your Data
  - Use Strong Passwords
  - Use Anti-Virus
  - Remote Access Requirements
  - Network Registration
  - Phishing/Social engineering
  - Protect computer and storage devices against theft
- **Some Ideas on protecting Information**
  - **Share with need to know basis**
  - **Vigilant about indirect questions**

Information Security

- **Generally information generated by organizations are open and accessible to anyone. Although some information may require review before it is released to the public, very little of this information requires protection.**
- **There are, however, a few special categories of information that require protection because of legal, contractual or safety requirements.**

Recognizing Official Media

- **Electronic media such as diskettes, removable hard drives, CDs, DVDs, tape cartridges, and thumb drives containing official information are marked with the words "Official Use Only"**

Floppy disc

Flash Drive

Access to Official Information is Restricted

- **Official information is not releasable to the public and must not be posted to web sites or other media.**

- **Access to Official information must only be provided to persons having a need-to-know the information to perform authorized activities.**

- **Official Information that is also marked Export Control Information should be restricted**

Protecting Official Information

- **While in Use**
- **Reasonable precaution must be used to prevent unauthorized physical, visual, and audio access to official use information.**
- **In Storage**
- ***Paper and other physical media* – official use information may be stored in unlocked receptacles, such as drawers and file cabinets, when internal building security, such as locked doors, is adequate to prevent unauthorized access when it is left unattended. Otherwise lockable receptacles must be used.**
- ***Electronic* - Computers and computer systems used for processing or storing official use information must provide security measures to prevent unauthorized access.**

Protecting Official Information

- **Reproduction**
- **Documents may be reproduced without permission of the originator to the minimum extent necessary. Copies must be marked and protected in the same manner as the original.**
- **Destruction**
- **Documents containing official use information must be destroyed by using a strip cut shredder producing strips no more than ¼ inch wide.**

Transmitting Official Information

- **Mail**
- **Always use a sealed opaque envelope, with the words "To Be Opened by Addressee Only."**
- **When mailing outside the Laboratory, ensure a return receipt address is supplied.**
- **Hand Carry**
- **Official Information may be hand carried between or within facilities provided the information can be protected from unauthorized access.**

Business Sensitive Information

- **Business Sensitive Information has the potential to damage organization, commercial, or private interests if disseminated to persons who do not need the information to perform their jobs.**
  - Such information may also be covered by a Nondisclosure Agreement (NDA) negotiated between organization and another party.
  - Commercial/proprietary information including trade secrets, business plans, and financial or cost data received from a company doing business, or contemplating business, with the organization
  - Intellectual property, contract negotiation information, procurement data, patentable design bids, and proprietary research and development information

Safeguarding and Handling Official and Business Sensitive Information-Good Practices

- **lock up all documents, removable media, laptops, and other media and materials containing this information when not in use.**
- **log off, turn off, or lock your computer whenever you leave your desk.**
- **destroy this information by shredding when no longer needed, if retention is not required.**
- **be conscious of your surroundings when discussing such data. Protect verbal communication with the same heightened awareness as you would paper or electronic data.**

Safeguarding and Handling Official and Business Sensitive Information

- **report poor information security practices relating to this information to your supervisor.**
- **immediately report any loss, unauthorized disclosure, or suspected security violation relating to this information to Security.**
- **submit scientific and technical information intended for publication for the required reviews for sensitive information and approval for release, before it is published, presented, or otherwise disseminated.**

Safeguarding and Handling Official and Business Sensitive Information

- **DON'T leave this information out and unattended.**
- **DON'T discuss, share, or entrust this information to individuals who are not authorized or who do not have a business need-to-know.**
- **DON'T post this information to web sites or other media.**
- **DON'T take home in either paper or electronic format.**

Why Do We Need Cyber Security Training?

- **People are the key component to protecting the confidentiality, integrity, and availability of the information and computing systems.**
- **A robust training and awareness program is essential to ensure people understand:**
  - Their responsibilities
  - The organization's cyber security policies
  - How to properly use and protect the information technology resources entrusted to them
- **All employees, and any visitor who requires an account and access to computing resources (whether local or remote access), must be aware of required security**

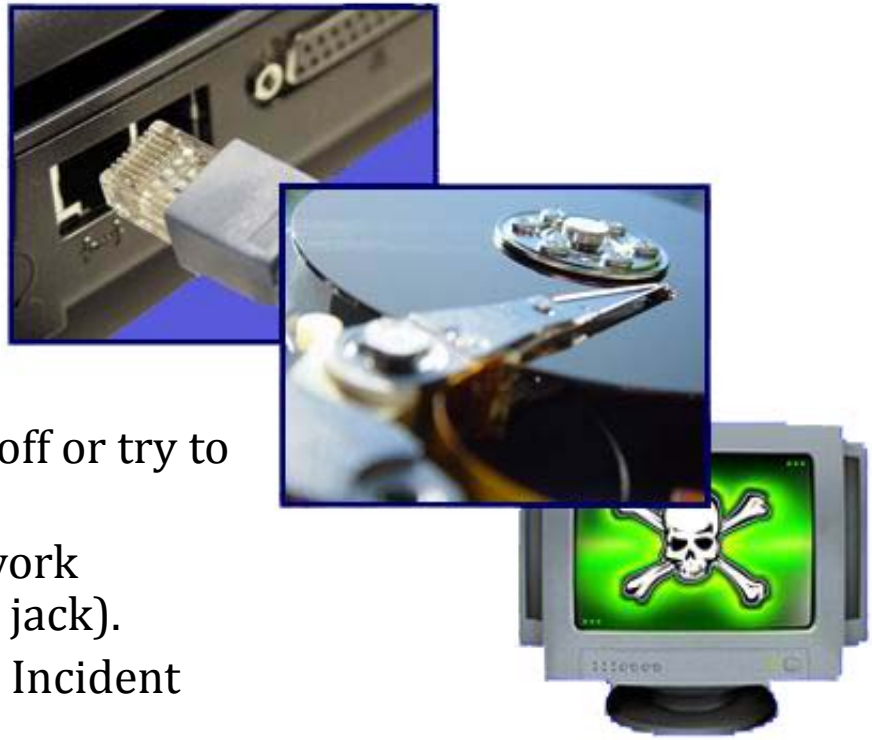
Elements of Cyber Security

- **Topics**
- **Incident Handling**
- **Physical Security**
- **Handling**
- **Social Engineering**
- **Standard Requirements**
- **Inappropriate Use**

Incident Handling

How to Identify and Report Potential Incidents

Whenever you identify an event that suggests suspicious activity, do the following:



- Stop using the system, but don't turn it off or try to clean it up.
- Disconnect the computer from the network (disconnect the network cable from the jack).
- Immediately contact the Cyber Security Incident Response Team

It's important for you to be able to recognize the types of signs that may indicate an intruder has accessed your computer system.

Signs of Intrusion or Attack

Strange occurrences, such as the following, may indicate a security breach.

- Unexpected access to disks
- Unexpected appearance of new files
- Unexplained increase in the usage of disk space
- Unexplained open applications
- Unexplained printouts of data
- Unexplained sluggishness in your system
- Unexplained user accounts
- Unexpected system log entries

An Example of the Type of Incident to Report

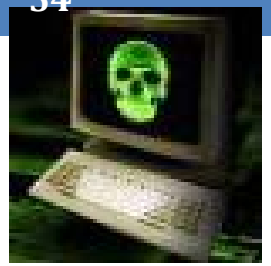
You receive an e-mail containing an unexpected attachment from someone you know, and feel safe opening the attachment because it's password-protected. (The password to open the file is included in the body of the e-mail message.)

- You open the attachment and your computer then becomes infected with a Bagle worm variant. Your newly infected system starts sending out e-mail messages to addresses from your address book.
- The next group of recipients also think the message they receive is from someone they know—you, so they open the attachment. In this way, the worm is spread to more and more computers under the guise of an e-mail from a known person.

The fact that an e-mail attachment was password-protected does not mean it is safe to open; in fact, the password-protected zip file is a clever ruse used by hackers to bypass e-mail scanners.

Instead of opening this unexpected e-mail attachment, the proper action to take would have been to contact s Cyber Security Incident Response Team.

Be Alert for Potential Viruses and Malware



- **Computer viruses, Trojans, worms, and malware are software programs deliberately designed to interfere with computer operations. These programs can destroy data, slow down your system, crash your system, steal your personal or critical information, and affect other users. These programs are usually spread via e-mail or by running programs that were downloaded from unknown sources.**

- **Be on the alert whenever you receive e-mail from unknown sources, download files from free download sites or copy files from unregistered media.**
  - Forward suspicious emails to security department
  - Do not open e-mail attachments from unknown sources.
  - Do not load software from illegitimate sources; the media could be infected with a virus, worm, Trojan, or malware.

Physical Security

Prevent Theft and Loss of Data

Always protect your computer from theft, whether you are on the Laboratory site, or traveling with a laptop. Report any missing computer or laptop immediately to security

Prevent Theft and Loss of Data

Lock your office when your computer is unattended for any reason and enable the password protected screensaver.

For Laptop Computers

- Computers that are used off site must be protected against theft and unauthorized use. Be careful when traveling with a laptop as airports and hotel lobbies are notorious places for computer theft.
- Don't pack a laptop in luggage that will be checked--always carry your laptop with you on the plane. Never leave your laptop unattended.
- Before taking your desktop/laptop computer off site, you must have an approved Offsite Property Pass.
- Don't save passwords that allow automatic login. (This prevents thieves from gaining access to your computer files and any associated sites if your laptop is stolen.)
- Full Disk Encryption must be used to protect any sensitive information stored on the system.

Social Engineering Attacks

What is Social Engineering and its Consequences?

Social engineering attacks can come in various forms:

- Phishing e-mails
- Helpdesk technician impersonators
- Phone calls asking for personal information or computer passwords
- Official-looking letters in regular mail threatening repercussions

The attacker's goal is to obtain information that will allow him/her to gain unauthorized access to your systems, assets, or personal information to use for their own purposes.

Consequences to you and BNL can be severe:

- Identity theft can cause long-term financial problems
- Compromised passwords can expose sensitive BNL resources to data theft
- Loss of personally identifiable information (PII) may result in publicly embarrassing newspaper articles and significant financial impact to the Laboratory
- Loss of research data could result in funding cuts, and compromised machines may cause disruption of services used by research collaborations

Guidance on Protecting Against Social Engineering

- **If you receive suspicious e-mail or phishing attempts, please contact Cyber Security at.**
- **If you are asked for your password over the phone, contact Cyber Security.**
- **If someone unknown or unexpected asks to work on your computer, please verify his/her identity**
- **If someone you do not know attempts to "piggyback" along when you enter a protected area, please contact Security**
- **Do not use portable media (USB memory sticks, CDs) from untrusted sources. It is now a common ploy for attackers to leave virus-infected USB devices lying around for the unsuspecting to find and put in their computers.**

Example: Phishing e-mail Received at BNL

From: Ucla Support Team [mailto:someuser@y7mail.com]
Sent: To: Joe, User
Subject: Confirm Your E-mail Address

Dear User,

We wrote to you on 28th February 2008 advising that you change the password on your account in order to prevent any unauthorised account access following the network intrusion we previously communicated. we have found the vulnerability that caused this issue, and have instigated a system wide security audit to improve and enhance our current security, in order to continue using our services you are require to update you account details below.

To complete your account verification, you must reply to this e-mail immediately and enter your account details below. Username: (**********) password: (**********)

Failure to do this will immediately render your account deactivated from our database. We apologise for the inconvenience that this will cause you during this period, but trust you understand that our primary concern is for our customers and for the security of their data. our customers are totally secure

Ucla Support Team

Module 3.2; Processes to safeguard information

- **Another important component of knowledge security is Establishing oversight personnel-Point of Contact**
  - Self-monitoring,
  - site POC,
  - peer review system,
  - implement through an established University/Institutional Review Board.

3. Processes to safeguard information

1. Know any research Funding Source Restrictions
2. R&D Contract Review and Oversight
3. Monitor Research Assignments and Equipment
4. Attention to Risks of Foreign Travel
5. Meaningful and Effective Export Control Program and Office
6. Emphasize Training and Education
7. Policy & Practice of Timely Self-Reporting Violations and taking Corrective Actions

Building an Integrated Knowledge Security Network

- **To be successful, knowledge security best practices must draw upon best practices from many areas**

Why is an Integrated Network needed?

- **As dual-use expertise spreads via many open sources, protection of specialized knowledge is needed**

- **Push from sciences: new technologies and new capabilities may increase the risk of proliferation of WMDs**

Information Security-Summary

At the completion of this section, you will be able to:

- **Describe your role and responsibilities in the Cyber Security program**
- **Detect, report, and properly handle intrusions on your computer**
- **Deter computer theft**
- **Be aware of "phishing" and other social engineering scams via e-mail, telephone, or in-person**
- **Understand the password complexity requirements and select a password that is difficult to crack**
- **Understand the importance of backing up data regularly and verifying the accuracy of data backups**
- **Register network devices accurately**

Multidimensional Proliferation Threats

- **Summary of threats:**
  - Threats posed by terrorism;
  - Threats posed by assimilation/state programs;
  - Potential threat posed by growing access to information by internet/social networking

- **'No single focal point' of threats**
  - Potential actors, material and information, which can be related to dual-use issues, exist at international, regional, national, local and individual levels.

From the Individual to the International

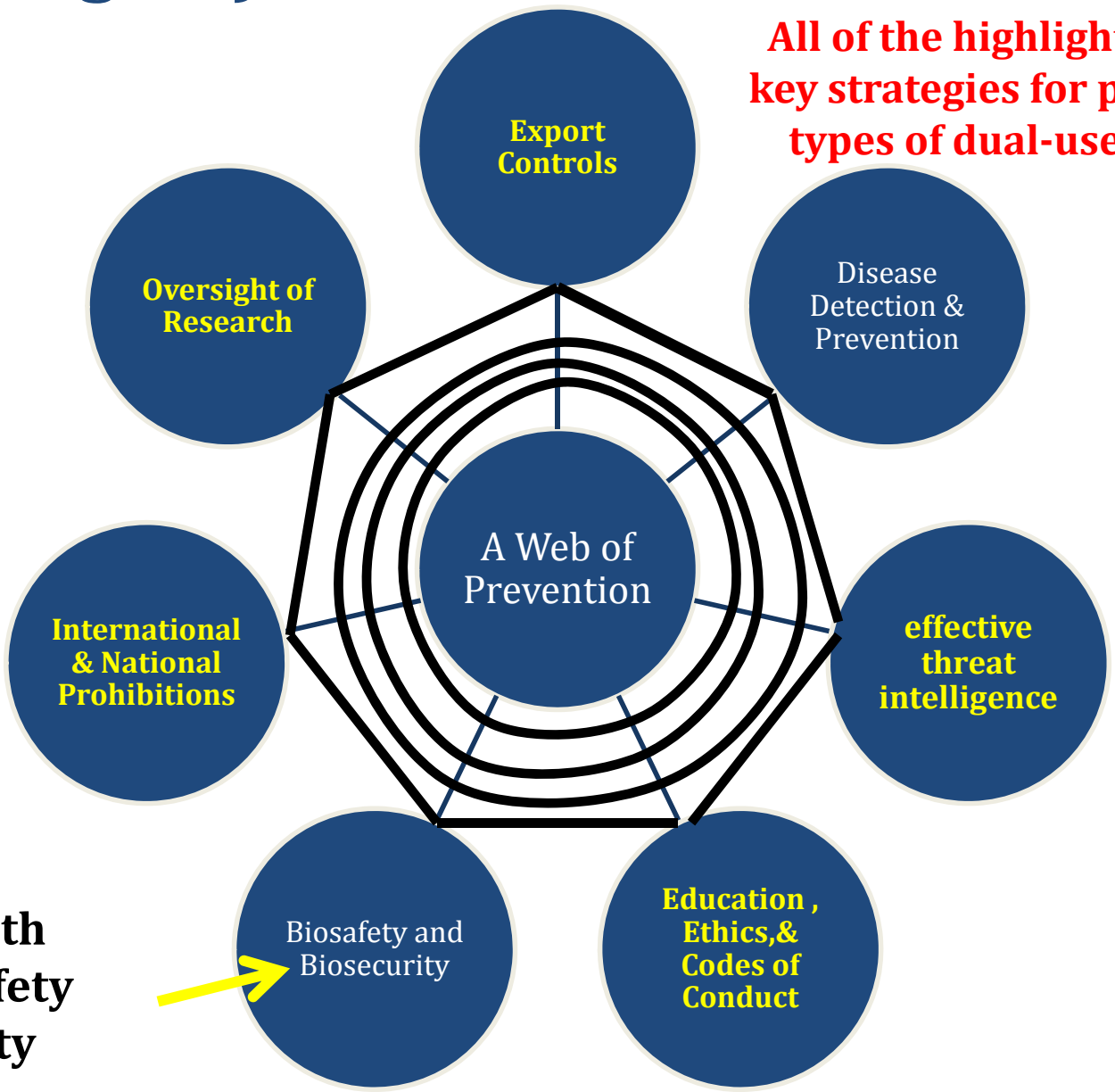
- ***The new reality is quite simple. Action is required at all levels; individual, sub-national, national, regional, like minded, and international, public, private, government and intergovernemental levels. Managing the biological weapons problems requires a rubric of measures from the individual to the international.***

Jez Littlewood

All dual-use, weapons-related information requires this level of attention, by the community who holds it.

The (Biological) Web of Prevention

All of the highlighted areas are key strategies for protecting ALL types of dual-use knowledge



Replace with unclear safety and security

The Need for Strong, Comprehensive Export Controls

- **Export controls are designed to ensure that exports do not contribute to the development of WMD**
- **Export controls should include provisions for agents, equipment and expertise**
- **Deemed Export laws can address intangible transfer of knowledge- yet this is VERY complex**

Awareness of International & National Prohibitions

- **The scientific/engineering community has responsibility to know their obligations under International prohibition regimes such as the NPT, CWC, UNSCR 1540, and the Geneva Protocol of 1925 as well as our country's specific, national measures to deter and dissuade individuals from contributing to the development of WMD**

- **For these obligations to be effective will require; education, broad implementation, and enforcement at every level- students, practicing scientists, management and government leaders.**

Education & Codes of Conduct

- **Education and codes function to raise nonproliferation awareness and knowledge security amongst the scientific community and deter those with the capacity to contribute to WMD**

- **There are a range of projects focused on education and codes in many countries…THIS COURSE IS ONE OF THEM**

- **This information and material can be used to TRAIN the PEERS**

Nuclear Security Culture- the Role of Knowledge Security

- **Many efforts under the umbrella of "Nuclear Security Culture" broadly promote measures and best practices to ensure nuclear energy is pursued safely and securely, and only for peaceful purposes**

- **Knowledge security- the protection of nuclear and dual-use knowledge is one component strengthening this larger security culture**

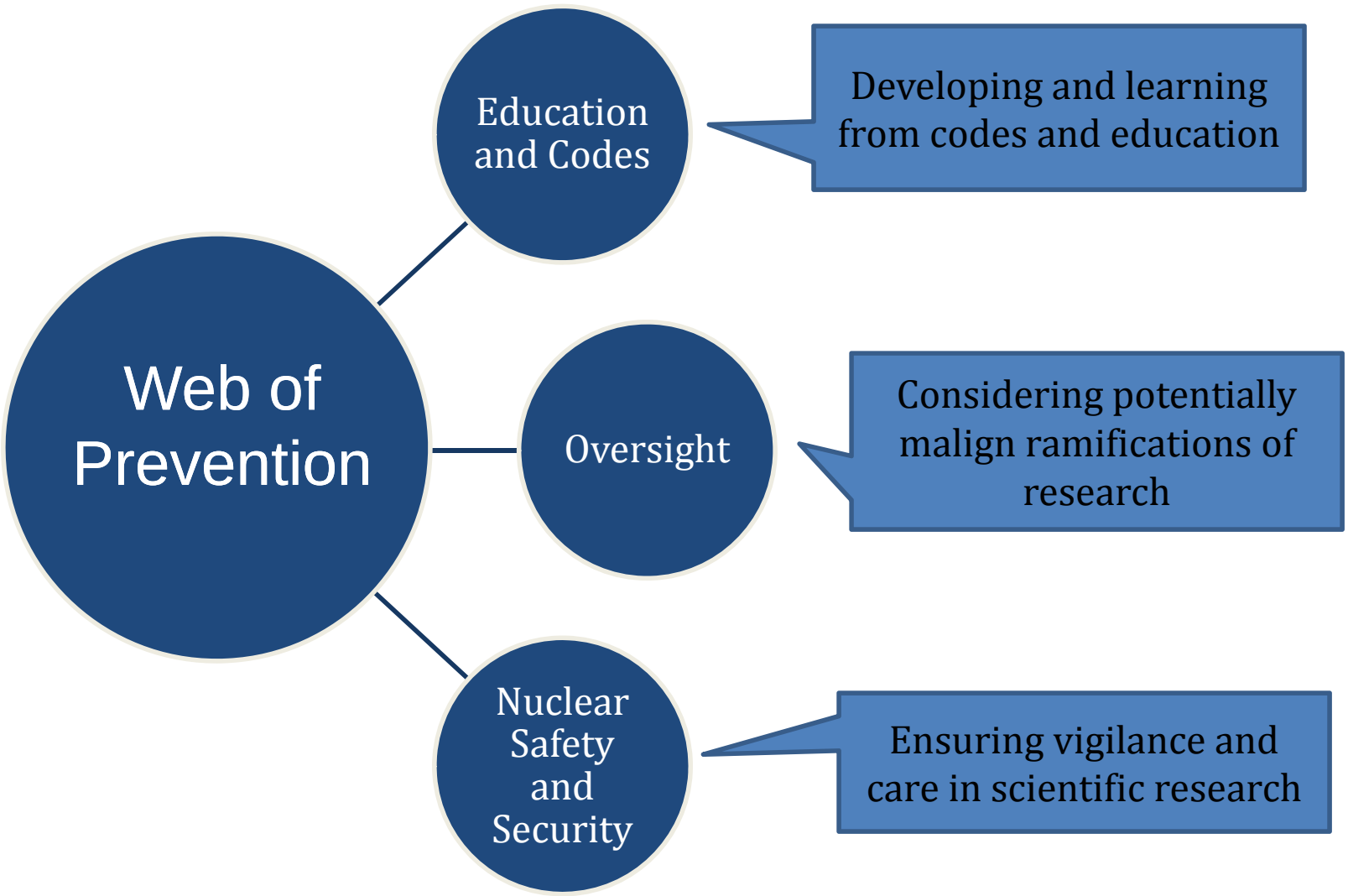
Oversight of Research Products

- **Science's main currency is the sharing of new technologies and information. Sometimes difficult to tell where to draw the line between what information to share, and what to withhold in a given situation**

- **Oversight personnel (your group leader, manager, independent review or peer board) can help determine the risks and proper action**

- **This is important in minimizing the possibility of sharing information that could cause unintentional harm by proliferation**

The Role of Scientists in the Web-Nuclear



EVERYTHING AFTER THIS SLIDE NEEDS TO BE RE_WORKED AND TAILORED TO OUR PURPOSES.

Acknowledgement- this is sourced from Biosecurity/bioethics best practices training materials – available for adaptation at FAS.or

Same themes, goals of this material material/messaging means we can re-interpret more broadly to other nuclear, dual-use audiences

Responsibility of Scientists associated with dual-use knowledge protection

Five criteria for the obligation to prevent harm. Researchers should strive to prevent harm that is:

- **Within their professional responsibility**
- **with their professional capacity and ability**
- **Reasonably foreseeable risk**
- **Proportionally greater than the benefits**

.

Duties associated with dual-use science

Those with dual-use expertise should strive to:

- **Consider the negative implications if their research is misused**

- **Systematically anticipate dual-use applications in your work in order to warn of dangers generated by them**

- **Not publish or share sensitive information**

- **Oversee and limit access to sensitive information**

- **Report activities of concern**

These obligations can be self-acknowledged and enforced, or codified into professional obligations of all workers/students

Information Dissemination and Security

- **This is an important issue and cause of conflict that confronts all scientists.**

- **Next few slides this issue will be further explored.**

Tensions in benefit and risk analysis

What is at stake are rights to academic freedom and scientific progress against the public's right to not be put at risk by the very research which is meant to help them.

"…secrecy strikes at the very root of what science is, and what it is for. It is not possible to be a scientist unless you believe that it is good to learn. It is not good to be a scientist, and it is not possible, unless you think that it is of the highest value to share your knowledge, to share it with anyone who is interested. It is not possible to be a scientist unless you believe that the knowledge of the world, and the power which this gives, is a thing which is of intrinsic value to humanity, and that you are using it to help in the spread of knowledge, and are willing to take the consequences." R, Oppenheimer, Los Alamos, NM Nov. 2, 1945

Tensions in benefit and risk analysis

"A common sense position is that trade-offs need to be made between rights to disseminate and scientific progress on the one hand, and security/public health needs on the other. On this view, we should sometimes be willing to make at least small sacrifices in the way of public health and/or security when this is necessary to achieve enormous benefits with regard to the progress of science; and we should sometimes be willing to make at least very small sacrifices with regard to the progress of science when this is necessary to achieve enormous benefits regarding public health and/or security."

Precautionary Principle For Individual

There are four main conceptual dimensions, which commonly occur in different versions of the precautionary principle : threat, uncertainty, prescription and action.

So that: "if there is (1) a threat, which is (2) uncertain, then some kind of (3) action is (4) mandatory".

Precautionary Principle

A Biosecurity-sourced precautionary principle can be applied for protection of all dual-use knowledge and information:

"When and where serious and credible concern exists that legitimately intended (biological) material, technology or knowledge in the life sciences pose threats of harm to human health and security, the scientific community is obliged to develop, implement and adhere to precautious measures to meet the concern."

Statement on Scientific Publication and Security

"We recognize that on occasion an editor may conclude that the potential harm of publication outweighs the potential societal benefits. Under such circumstances, the paper should be modified or not be published. Journals and scientific societies can play an important role in encouraging investigators to communicate results of research in ways that maximize public benefits and minimize risks of misuse."

Statement on Scientific Publication and Security

"The Statement claims that editors may sometimes make censorship decisions, but it gives no reasons for thinking that editors, or the scientific community in general, for that matter, are especially qualified to judge security risks. An important question thus concerns the extent to which the government, bioethicists and/or the security community should be involved in scientific censorship."

Decision making for dual-use dilemmas

- **Complete autonomy of individual scientist**
- **Institutional control**
- **Mix of institutional and governmental control**
- **An independent authority**
- **Full governmental control**

Decision making for dual-use dilemmas

Most bioethicists believe that only a mixed authority which is constituted by the scientific community together with government bodies can address the dual-use dilemma.

Determining who is responsible in a given case will be "context dependent".

MODULE 3.3 Group Exercises

Module 3.3; Group Discussion and Exercise

- **What can I do as an individual to protect my knowledge?**
  - Today
  - In the near future
  - Throughout my career

- **What can my (institute/university) do?**
  - Oversight personnel?, Peer review system
  - Code of Conduct/Internal compliance program
  - Provide resources and information on sharing of information, to help make informed decision

- **What can my government do?**
  - Laws (deemed export)

Group Discussion and Exercise

- **Building a code of conduct- Discussion**
  - Leverage with UK CoC materials?
- Much has been written about codes of conduct in science and engineering. Many questions have been or need to be raised. The most important goal is to get scientists and students continually involved in developing their own codes. These would address questions such as:
- **- Are explicit codes really needed? If so, what types of codes? - Are they effective, and at what?**
  - Is a code the most appropriate way to secure high standards of behaviour?
  - How can codes be made relevant and alive?
  - Could one ethical code be expected to be universally valid?
  - Do codes have a widespread appeal outside of the countries where they have been developed?
  - Who should devise codes?

Group Discussion and Exercise

- **Building a code of conduct- Questions to discuss with group:**

- What would it have in terms of its content?
  - What would it say about scientists and engineers considering the implications of their work?
  - Would it aim simply to inspire? Or should it provide clear guidelines for appropriate conduct?
  - What would it say about the need to prevent the spread of chemical weapons?
  - What would it say about the need for responsible utilization of multi-use chemicals like ephedrine?
  - Who would be its primary audience?
  - In an ideal world, who would be involved in its development?
  - How could it be disseminated and made relevant to those in science and engineering and possibly beyond?

Module 3.4; WEB based Platform-Resources and Community

MODULE 3.4; WEB Based Platform

- **Create a WEB based platform to provide access to resources; course material, references and links**
- **WEB based Frequently asked Questions**
- **WEB Based Forum for discussion and creation of non-proliferation community**
- **WEB to be hosted at DOE National Lab with open access.**

Module 3 Summary

- **List key concepts**
- **Questions and Discussion**

Final Thoughts, Closing of Course

- **Review course, feedback**
- **Points for further work**
- **Questions and Discussion**