Attending a Joint Certification Program (JCP) Controlled Conference where a DD Form 2345 certification number is required

Background:

In 1985, the United States and Canada signed a Memorandum of Understanding (MOU) that established the U.S.-Canada Joint Certification Program (JCP). The MOU stated that the JCP was established to "certify contractors of each country for access, on an equally favorable basis, to unclassified technical data disclosing critical technology" controlled in the U.S. by the Defense Directive 5230.25 and in Canada by the Technical Data Control Regulations. The JCP is managed by the U.S-Canada Joint Certification Office (JCO) which is located in the Defense Logistics Information Service (DLIS). JCO receives and processes the DD Form 2345, Military Critical Technical Agreements, submitted by U.S. and Canadian contractors who wish to obtain access to unclassified technical data disclosing critical technology under the control of the U.S. Department of Defense or the Canadian Department of National Defense.

In order to attend a meeting or conference where unclassified technical data will be disclosed, a JCP certification number is required. The U-M holds an approved Military Technical Data Agreement DD Form 2345. The U-M Export Control Officer can provide you with the JCP certification number listed on the DD2345.

What is unclassified technical data?

It is governed in the U.S. by Department of Defense directive 5230.25. It can include any of the following:

- Technical data with military or space applications
- Any blueprints, drawings, plans, instructions, computer software or documentation
- Other technical information that can be used or be adapted for use to design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning such equipment

I've been invited to attend a meeting/conference, what do I need to do?

You should obtain the JCP certification number from the U-M Export Control Officer at exportcontrols@umich.edu

You should attend the conference in your capacity as a U-M employee and use the U-M JCP Certification number.

You should be aware that access to unclassified technical data is controlled and may not be exported outside of the U.S. without an approval authorization or license under U.S. or Canadian export control

laws. This also means that you cannot share any unclassified technical data with any foreign nationals here in the U.S.

When you return from your meeting/conference, you should contact the U-M Export Control Officer if you brought any unclassified technical data or anything labeled "export controlled" back with you from the meeting/conference.

In the future, materials may be mailed to the U-M Export Control Officer related to your attendance at the meeting/conference. If that happens, you will be contacted to determine if you would like access to the materials. If so, a Technology Control Plan (TCP) may need to be put in place to be sure no foreign nationals will have access to the materials.

ACCESS TO MILITARY CRITICAL DATA – FORM DD2345

ACKNOWLEDGEMENT AND USE OF FORM

A certification is required by U.S. or Canadian contractors that wish to obtain access to unclassified technical data disclosing militarily critical technology with military or space application that is under the control of, or in the possession of the U.S. Department of Defense or the Canadian Department of National Defence. Certification under the Joint Certification Program is the sole method to establish the eligibility of a U.S. or Canadian contractor to technical data governed, in the U.S., by DoD Directive 5230.25 and, in Canada, by the Technical Data Control Regulations.

The University of Michigan has submitted the required documentation to the JCP to obtain a certification for access to such information. This certification is maintained and controlled by the Export Control Officer (ECO) in the ECO's role as an Empowered Official for the University and for the ultimate end-use of University faculty and staff upon written request to the ECO. All such requests for usage of the University DD2345 Certification are subject to the review and approval at the discretion of the ECO. Any approval is subject to the following provisions which must be accepted in writing by the requesting user prior to release of a copy of the Certification Form to the user.

This request for use of the University DD2345 is related to the following anticipated activities only:

Access to Military Critical Information for other purposes must be approved under a separate request.

Specific Security Provisions:

1. Transmission of military critical technical data or information from the source to the University may require delivery directly to the ECO. User understands and acknowledges that, in the event such transmissions are received, the ECO may delay delivery as necessary to prevent any unauthorized disclosures and/or disclosure risks and a Technology Control Plan may be required.

2. User must contract the ECO if any documents are received under this DD22345 so that a Technology Control Plan may be immediately put in place. Documents received by User which are marked as controlled, restricted, sensitive or otherwise not intended for general access or release must be kept in a restricted access format:

    a. For hardcopy files, materials shall be kept in a secured location (such as, a locked desk, file cabinet, office) to which unauthorized and unsupervised access is not provided to third-parties;

    b. For electronic data and records, all items shall be stored in an encrypted manner to maintain IT security as further described below.

General Computer Security Provisions:

1. All computers onto which any covered technical data shall be installed that are connected to the internet or other unsecured networks must be protected behind appropriately configured security appliances (i.e., firewalls).

2. All computers onto which any covered technical data shall be installed will have all relevant security patches applied.

3. Any electronically stored copies of any covered technical data shall be stored in an encrypted format using, at a minimum, a password decryption mechanism for access.

Document Management and Disposition Security Provisions:

1. University computer security policies and procedures will be followed.

2. Upon conclusion of the need for access to any covered technical data, all covered technical data shall be destroyed, removed, and/or returned to the original source.

Acknowledgement by University Requesting User of these provisions and obligations:

_____	_____	_____
Printed Name	Signature	Date

_____	_____	_____
Affiliation with University	Department	Citizenship/Permanent Residency Status

Questions regarding Export Compliance should be directed to the Export Control Officer at exportcontrols@umich.edu.