May 20, 2004

Janice Pesyna
Office of the General Counsel
Department of Homeland Security
Washington, DC 20328

RE: **Procedures for Handling Critical Infrastructure Information**
(6 CFR Part 29; RIN 1601–AA14)

Dear Ms. Pesyna,

The Michigan Credit Union League (MCUL) appreciates the opportunity to provide comments to the Department of Homeland Security (DHS) concerning the DHS's procedures for handling critical infrastructure information (CII). The MCUL is a trade association representing over 90% of state and federally chartered credit unions in the state of Michigan. This comment letter was drafted in consultation with the MCUL Government Affairs Committee, which is comprised of Michigan credit union staff and officials.

MCUL supports the DHS' ability to gather important infrastructure information to better protect U.S. businesses. We believe that any effort to curb terrorism and better protect the United States against possible attacks to our infrastructure is worthwhile. We support the voluntary submission of this information with the following suggestions to better improve the system to encourage more credit unions to provide this data.

Summary of Comments

- We believe the following procedures would improve the level of acceptance for indirect submissions. 1) Provide notification to the entity involved prior to the submission of information; 2) Authorization from these entities that their information may be shared with other government agencies; 3) An opt out provision to allow private sector entities to keep their information private; 4) An agreement that information provided by other entities will not be used for any other purpose than expressly spelled out by DHS; 5)
- We would like the following to be included in the final rule to encourage credit unions and other private sector entities to share CII:
    - Would like to have the DHS create model forms for submission so that there would not be any confusion if information were classified.
    - If the Protected CII Program Manager or the Manager's designee(s) make an initial determination that the information submitted does not meet the requirements of Protected CII, they must notify the submitter. Along with the other reason's proposed to be explained, we believe they should explain why the information does not meet the requirements.
    - Protected CII may be provided to foreign governments to the same extent and under the same conditions it may provide advisories, alerts and warnings to state and local

governmental entities, or in furtherance of an investigation or in prosecution of a criminal act. We would like to know what assurances do we have that other foreign governments will protect the information.
    - Criminal and administrative penalties may be imposed on a federal government employee who knowingly publishes, divulges, or makes known to any extent not legally authorized any information protected from disclosure under the CII Act. We would like for there to be a provision that any expenses relating to the reconstruction of critical infrastructure caused by this employee be paid by the agency responsible for the loss.
- We feel the interim rule is sufficiently flexible to allow DHS to adapt as the Protected CII Program evolves, however we would like any new provisions to be published as a request for comments to allow industry input from those entities most affected.

Discussion

Indirect CII Submissions. MCUL understands the comments that DHS received which expressed concern regarding the provision enabling indirect submissions. We appreciate the references to indirect submissions being deleted from the interim rule. We believe that indirect submissions may be a possible alternative in the future, but first there would need to be checks and balances put in place to ensure the information provided is not used for any purposes other than what is intended. The following are our recommendations:

We believe the following procedures would improve the level of acceptance for indirect submissions.

1. Provide notification to the entity involved prior to the submission of information. We believe that all entities should be notified prior to any information being provided about them. They should have a reasonable period to respond if they have reasons for not wanting that information to be shared.
2. Authorization from these entities that their information may be shared with other government agencies. Each entity should have the authority to determine whether or not their information is shared with others. This will prevent the random sharing of information among government agencies, since this information is provided voluntarily. We want to ensure that any information provided from one agency to the next is done so for valid reasons.
3. An opt out provision to allow private sector entities to keep their information private. We would like for there to be an automatic "opt out" form that will prevent one agency from providing information to another. This could be provided at the time they submit their voluntary information. This would encourage more credit unions to provide proprietary infrastructure information to the DHS.
4. An agreement that information provided by other entities will not be used for any other purpose than expressly spelled out by DHS. All entities that are allowed access to this information should be required to sign documentation that they will not use the information provided for any other reason than what is expressly stated in the agreement. Any entity that voluntary submits information for one purpose should not be concerned that this information will be used by another entity to their possible detriment in the future.

Additional Protective Measures to Encourage Sharing CII. We would like the following to be included in the final rule to encourage credit unions and other private sector entities to share CII:

Would like to have the DHS create model forms for submission so that there would not be any confusion if information were classified. Creating designated forms that pertain all of the necessary disclosures, including the disclosure: "This information is voluntarily submitted to the Federal government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002." This would alleviate concerns from credit unions as to whether or not they included all necessary information to prevent the information from being shared with others.

It could also provide basic questions on it to help a credit union determine if the information would fall under protected CII and would improve the submission process. It could also have any explanations or disclosures that DHS would have to provide to indicate when information is no longer considered Protected CII. This would include when the Protected CII Program Manager of the Manager's designee(s) determine that the information was customarily in the public domain, is publicly available through legal means, or is required to be submitted to DHS by federal law or regulation.

If the Protected CII Program Manager or the Manager's designee(s) make an initial determination that the information submitted does not meet the requirements of Protected CII, they must notify the submitter. Along with the other reason's proposed to be explained, we believe they should explain why the information does not meet the requirements. This would help credit unions to understand why their information is no longer protected. Without providing this information, we believe that credit unions would not have the necessary information available to determine if they should continue to submit CII to the DHS. They may believe that these decisions are of a capricious or arbitrary nature.

Protected CII may be provided to foreign governments to the same extent and under the same conditions it may provide advisories, alerts and warnings to state and local governmental entities, or in furtherance of an investigation or in prosecution of a criminal act. We would like to know what assurances do we have that other foreign governments will protect the information. Technology not only allows a great deal of information to be accessed by basic computer systems, but it allows that information to be accessed remotely, including from foreign countries. The laws protecting our information in the United States do not extend across our borders. We would like to know what barriers are in place to prevent important CII information from being leaked by foreign governments into the wrong hands. With credit unions especially prone to identity theft through the use of information found on computers, this is of particular concern.

Criminal and administrative penalties may be imposed on a federal government employee who knowingly publishes, divulges, or makes known to any extent not legally authorized any information protected from disclosure under the CII Act. We would like for there to be a provision that any expenses to the entity relating to the reconstruction of critical infrastructure caused by this employee be paid by the agency responsible for the loss. If critical CII is leaked which would cause a credit union to dramatically change their infrastructure information for purposes of protection to their members, it can be very expensive. If credit unions are voluntarily providing this information to the DHS, and it is leaked, then it should be the responsibility of DHS or the department from which the employee worked, to compensate the entity to get them back to a secure state. This would serve to alleviate some concerns over providing such information.

Encourage Flexibility with Industry Input. We feel the interim rule is sufficiently flexible to allow DHS to adapt as the Protected CII Program evolves, however we would like any new provisions to be published as a request for comments to allow industry input from those entities most affected. We are concerned that before DHS change any of its procedures that it first consult with those whom it will affect. We want DHS to be flexible enough to continue their fight against terrorism, however we do not want that to be at the expense of the rights of credit unions. We ask that any changes the DHS contemplates in their procedures regarding the use of CII require notification prior to implementation.

We thank you for the opportunity to comment.

Sincerely,

Matthew Beard
Regulatory Specialist
Michigan Credit Union League

cc: Credit Union National Association, Inc.