OPSEC PROGRAM SELF-EVALUATION CHECKLIST

Answer yes, no, or not applicable (NA) to each of the items on the checklist. Some questions repeat with slight variation as you move to the next tier. Each tier assumes the accomplishment and sustainment of prior tier requirements.

1. Tier One OPSEC Programs. NOTE: If all items are “yes”, go to Tier Two.			
ITEM	YES	NO	NA
1.1. Has an OPSEC Program Manager been appointed?			
1.1.1. Is there an appointment letter?			
1.1.2. Has the appointment been announced?			
1.2. Does the OPSEC Program Manager dedicate between 10% and 30% of available duty hours to OPSEC?			
1.3. Has leadership signed a local policy letter?			
1.3.1. Has the letter been distributed to all managers/supervisors?			
1.3.2. Are all personnel aware of the policy?			
1.3.3. Is the policy periodically reviewed for currentness and updated as necessary?			
1.4. Has leadership appointed an OPSEC Working Group?			
1.4.1. Does the Working Group meet periodically?			
1.4.2. Is the role of the Working Group clearly defined?			
1.4.3. Have all Working Group members been trained?			
1.4.4. Are Working Group members who leave the organization replaced?			
1.4.5. Is there a mechanism in place to train new Working Group members?			
1.5. Has a Critical Information List (CIL) been published?			
1.5.1 Has the CIL been approved by leadership?			
1.6. Does the organization have an awareness training program?			
1.6.1. Are all newly assigned personnel trained within 90 days of assignment?			
1.6.2. Do all personnel receive awareness training at least annually?			

NOTES:

2. Tier Two Programs. NOTE: If all items are “yes”, go to Tier Three.			
ITEM	YES	NO	NA
2.1. Does the Program Manager dedicate 30% to 50% of available duty hours to OPSEC?			
2.2. Does the Working Group meet quarterly?			
2.3. Have all Working Group members been trained?			
2.4. Are Working Group members who leave the organization replaced?			
2.5. Is there a mechanism in place to train new Working Group members?			
2.6. Are all newly assigned personnel trained within 60 days of assignment?			
2.6.1. Has leadership established frequency requirements for workforce awareness training?			
2.7. Has the OPSEC Program Manager prepared an OPSEC plan?			
2.7.1. Is the plan signed by leadership?			
2.7.2. Has the plan been distributed to all managers/supervisors?			
2.8. Does the Program Manager keep a continuity book or file?			
2.9. Is senior leadership actively involved in the OPSEC program?			
2.9.1. Participates in awareness training?			
2.9.2. Addresses OPSEC issues in all-hands meetings?			
2.9.3. Regularly includes OPSEC concerns in senior staff meetings?			
2.9.4. Requires OPSEC input to planning and special events?			
2.10. Have OPSEC coordinators been assigned in accordance with local policy?			
2.10.1. Does the Program Manager meet regularly with coordinators?			
2.10.2. Is the role of the coordinator clearly defined?			
2.10.3. Have all coordinators been trained?			
2.10.4. Are coordinators who leave the organization replaced?			
2.10.5. Is there a mechanism in place to train new coordinators?			
2.11. Does the Program Manager have a plan to use end-of-year money?			
2.12. Is a survey or assessment conducted at least annually?			
2.13. Has the Program Manager developed a support network to include:			
2.13.1. Counterintelligence specialists?			
2.13.2. Appropriate security specialists, such as IT and communications security?			
2.13.3. Threat analysis experts?			
2.13.4. Other OPSEC experts?			

NOTES:

3. Tier Three Programs			
ITEM	YES	NO	NA
3.1. Does the Program Manager dedicate 70% to 100% of available duty hours to OPSEC?			
3.2. Are all newly assigned personnel trained within 30 days of assignment?			
3.3. Do all personnel receive awareness training at least quarterly?			
3.4. Does the Program Manager document all organizational OPSEC training?			
3.5. Does the Program Manager contribute to the local newsletter (electronic or print)?			
3.5.1. Are copies maintained with the OPSEC program records?			
3.6. Does the Program Manager conduct self-evaluation quarterly?			
3.7. Is a survey or assessment conducted at least once annually?			
3.7.1. Are countermeasures implemented to correct vulnerabilities?			
3.8. Is OPSEC incorporated in local exercises?			
3.9. Is the Program Manager part of the emergency action team?			
3.10. Does leadership require OPSEC support for contingencies or emergencies?			
3.11. Is OPSEC incorporated into standing operations plans?			
3.12. Does leadership have written policies on the use of secure communications?			
3.13. Does the Program Manager have input to web content management?			
3.14. Does leadership request COMSEC monitoring at least once annually?			
3.15. Does the OPSEC program have a budget for training and awareness materials?			

NOTES: