METADATA SECURITY CHECKLIST

- Establish companywide (not individualized or optional) security policies to identify and tag metadata-sensitive projects and work product that could harm the company or its clients' and customers' interests if the metadata were to be disclosed. Require security verification of the metadata for security-tagged electronic work product prior to release.
- Train personnel to be aware of the potential liability for any disclosure of metadata: the legal discovery implications, the ethical requirements to preserve client confidentiality and other privileged information, and the potential malpractice for impairing client or firm interests.
- Ensure that personnel know how to view and to remove metadata in electronic files; companywide technical advice and assistance should be available.
- Use an "ESI discovery team" to direct and monitor all identification, screening, and production of ESI in response to litigation discovery requests.
- Be ready to alert clients to the forensic implications of metadata for potential legal and evidentiary exposure—for example, backdated stock options or revisions to bids or proposals.